APPENDIX G

ENTERPRISE IT STANDARDS

Commonwealth of Pennsylvania

Department of Transportation

Enterprise Information Technology Standards

Guiding Principles, Technical Architecture Guidelines,
Reference Architectures, Enterprise Solutions, Enterprise Infrastructure,
Standard Technologies & Hosting Requirements

Version 5.4
Effective: March 23, 2017

EASM
Enterprise Architecture
& Service Management

pennsylvania
DEPARTMENT OF TRANSPORTATION

Table of Contents

1 Document Information

1.1 Purpose

This document has been developed by PennDOT's Enterprise Architecture and Service Management (EASM) program to document, achieve consensus and communicate the organization's Enterprise IT Standards.

1.2 Intended Audience

This document is to be used by technical professionals (e.g. infrastructure and application architects, server engineers and administrators, etc.) who participate in the design, development, maintenance and support of IT solutions for PennDOT. IT managers, project managers, business analysts and others in the broader IT community will also find this document useful for a wide range of activities, including: portfolio and project planning, requirements analysis, etc.

This document is made available to PennDOT and other Commonwealth employees, contractors, business partners and prospective contractors.

1.3 Intended Use

PennDOT's EASM program will facilitate the use of this document in promoting technology, solution and architecture standardization and rationalization. The intended uses for this document include but are not limited to the following:

- Communicating enterprise standard technologies, solutions and architectures to IT stakeholders,
- Evaluating proposed technical architectures,
- Providing guidance for the technical architecture of new and significantly updated IT solutions,
- Providing guidance to potential vendors regarding requirements and standards when creating responses to requests for proposals and quotations (RFPs and RFQs), and
- Providing guidance to PennDOT staff when evaluating RFPs and RFQs and other procurement related documents.

1.4 Contents of This Document

Section 1 Document Information provides basic document information, including the purpose, intended audience and intended use as well as a brief description of the contents. *Section 2 IT Standards in Practice* provides information about the different types of IT standards defined at PennDOT and the processes for applying these standards to ensure optimal technical architecture for our IT solutions. Sections 3 through 9 define PennDOT's actual Enterprise IT Standards in the form of Guiding Principles, Technical Architecture Guidelines (TAG's), Reference Architectures, Enterprise Solutions, Enterprise Infrastructure, Enterprise Technologies and Hosting Requirements.

1.5 Revision History

Date	Version	Author	Description of Change
11/28/2012	1.0	Don Kirschman	Initial draft of the document
12/10/2012	1.1	Don Kirschman	Added Section for *Reference Architectures*. Also, minor edits throughout document based on EASM feedback.
12/12/2012	1.2	Don Kirschman	Added section for *Enterprise Solutions*. Formatting and minor content changes throughout the document.

Date	Version	Author	Description of Change
12/18/2012	1.3	Don Kirschman, Gautam Ray	Content and formatting edits to all sections of the document. Added section on Changing Standards.
1/7/2013	1.4	Don Kirschman	Removed references to *Platform Technologies* and adopted the term *Enterprise Technology* for consistency with ITLM. Added content to *Reference Architectures*. Made various other changes throughout the document.
1/10/2013	1.5	Don Kirschman	Added content to: Section 1.6 Architecture Evaluation, Section 1.7 Waivers from Standards and Section 2.2 Standard Enterprise Solutions. Changed cover page, headers, footer, etc. Formatted all tables consistently and other minor format and content changes throughout the document.
1/22/2013	1.6	Don Kirschman	Broke Section 2 into Sections 2, 3 and 4. Added content from *IT Infrastructure Guidelines* and *BIO Systems Environment* documents as Sections 5 and 6 respectively. Added “Contents of This Document” to Section 1. Updated EASM logo.
2/11/2013	1.7	Don Kirschman	Added section on COTS and IT Standards. Changed IT Infrastructure Guidelines to Guiding Principles for Technical Architecture. Added Guiding Principles regarding Java/.NET and relational databases. Other minor changes.
3/6/2013	2.0	Don Kirschman	Removed Appendix B and Appendix C the IT Solution Architecture Evaluation form and the IT Standards Waiver Request form, respectively.
3/26/2013	2.1	Don Kirschman Gautam Ray	Moved Guiding Principles upfront immediately following General Information. Added new Guiding Principles. Modified some of the existing Guiding Principles.
3/27/2013	2.2	Don Kirschman	Renamed Section 1.9 to “Deviations from Standards” and removed all verbiage concerning waivers.
4/22/2013	2.3	Don Kirschman	Incorporated suggestion regarding timing of COTS evaluation and accepted changes on several minor typographical edits throughout the document.
5/10/2013	2.4	Don Kirschman	Incorporated changes to align with ITLM process as well as dozens of minor grammar, spelling and content changes throughout the document.
8/11/2013	3.0	Doreen Wallen	Added Section 5.5 reference architecture for mobile applications.
10/9/2013	3.1	Don Kirschman	Added Section 5.6 reference architecture for Domino applications and Section 5.7 reference architecture for SharePoint applications.
6/10/2014	3.2	Don Kirschman	Changed 3.1 to indicate Enterprise Technology Inventory report from ITLM is report ITLM008. Expanded some descriptions of Enterprise Solutions. Various grammar, spelling and format corrections/changes.

Date	Version	Author	Description of Change
7/21/2014	4.0	EASM Team	Updated to incorporate external documents and strengthen wording to reflect standards concept.
12/11/2014	4.1	EASM Team	Edits made based on Joyce B., comments. See document outlining questions and comments. In addition hosting requirements section has been entirely updated.
05/11/2015	4.2	EASM Team	Changed Section 6 to remove versions for technologies listed in Standard Enterprise Technologies section. Updated Section 3 with newest PennDOT Enterprise Software Inventory.
6/16/2015	4.3	ITLM Process Owner	Updated Section 3 Standard Enterprise Technologies with current Enterprise Software Inventory
8/12/2015	4.4	ITLM Process Owner	Updated Section 3 Standard Enterprise Technologies with current Enterprise Software Inventory
9/10/2015	4.5	ITLM Process Owner	Updated Section 3 Standard Enterprise Technologies with a newly renamed PennDOT Enterprise Technology Standard report (ITLM008). Changed references to old report name Enterprise Software Inventory.
4/27/2016	4.6	ITLM Process Owner	Updated Section 3 Standard Enterprise Technologies with current PennDOT Enterprise Technology Standard report (ITLM008).
6/3/2016	5.0	Don Kirschman	• In Section 2, edited and expanded material concerning the types of Enterprise IT Standards, adding the concept of Technical Architecture Guidelines (TAG's) and Enterprise Infrastructure as types of standards. • In Section 2, consolidated and expanded material that defines how standards are developed and how they are used/applied on IT projects to effect a more optimal EA. • Added a new section (Section 3) exclusively for the Guiding Principles for Enterprise Architecture. • Added a new section (Section 4) for TAG's and added new TAG's for General Technical Architecture (ARCH), Enterprise Application Integration (EAI), Data Architecture (DATA) and Identity & Access Management (IAM). • Added a new section for Reference Architectures (Section 5) for the architectures that were defined as part of the Legacy Modernization project. • In Section 5, updated the "placemat" Reference Architecture diagram to have less technical granularity and more high-level classification and clarification information. • Renumbered sections as needed due to new sections that were added. • Relocated Enterprise Technologies towards the back of document (now Section 8). • Changed the document template formatting.

Date	Version	Author	Description of Change
7/20/2016	5.1	Don Kirschman, Gautam Ray, and Nathan Balagopal	• Updated Reference Architecture (Section 5) to add bullet points to further define the placemat reference architecture diagram. • Incorporated additional perspective diagrams provided by BIO/Nathan B. into the Reference Architecture (Section 5).
8/5/2016	5.2	Don Kirschman Rob Mohler	• In Section 8.2, incorporated latest version of Enterprise Technologies from ITLM008 report to reflect updates made to ITLM technology inventory.
2/2/2017	5.3	Paul Joseph	• Inserted to section 7 Enterprise Infrastructure, section 7.5 URL Branding – Application Web Site Naming Convention (DNS)
3/21/2017	5.4	Don Kirschman, ITLM Process Owner	• Updated Runtime Reference Architecture diagram (WMB changed to IIB). • Updated Section 8.2 with the latest technology standard listing with updated ITLM008 report.

2 IT Standards in Practice

2.1 Types of IT Standards

PennDOT's EASM program has established a set of *Enterprise IT Standards* to ensure a business-driven EA from the top-down and an optimized, responsive and flexible EA from the bottom-up. The seven types of *Enterprise IT Standards* are:

1. *Guiding Principles for Enterprise Architecture* – Defined in Section 3,
2. *Technical Architecture Guidelines* – Defined in Section 4,
3. *Reference Architectures* – Defined in Section 5,
4. *Enterprise Solutions* – Defined in Section 6,
5. *Enterprise Infrastructure* – Defined in Section 7,
6. *Enterprise Technologies* – Defined in Section 8, and
7. *Hosting Requirements* – Defined in Section 9.

2.2 Applicability of IT Standards

These *Enterprise IT Standards* are generally and broadly applicable to any IT solution that:

- Is developed by or for PennDOT,
- Is hosted in PennDOT or Commonwealth environments, or
- Is or will be supported by PennDOT IT resources.

In addition to PennDOT's Enterprise IT Standards, solutions that meet the criteria above must also comply with all Commonwealth standards defined by the Office of Administration/Office for Information Technology (OA/OIT) in Information Technology Policies (ITP's).

No comprehensive set of IT standards can be 100% applicable for all solutions or projects. The extent to which these standards apply varies depending on the scenario as defined by the development, hosting and support models for the solution. The table below presents some common scenarios and the corresponding level of applicability of the *Enterprise IT Standards*.

Scenario	Applicability of IT Standards
PennDOT Developed and Supported: PennDOT resources (staff and internal consultants) develop a custom application, provide application maintenance and support, and host it in PennDOT and/or Commonwealth environments.	**High:** The solution shall comply with all relevant standards in all sections of this document.
3rd Party Developed, PennDOT Supported: PennDOT has a 3rd party develop a custom application (e.g. RFP/RFQ, etc.), the application is or will be transitioned to PennDOT resources for application support and maintenance, and the application is hosted in PennDOT and/or Commonwealth environments.	**High:** The solution shall comply with all relevant standards in all sections of this document with the exception that use of enterprise application frameworks (e.g. PDJF) shall be considered preferred but not mandatory.
COTS PennDOT Hosted: PennDOT procures a generally-available COTS product with minimal or no customization and hosts the application in PennDOT and/or Commonwealth environments.	**Medium:** The solution shall comply with standards related to Operating System, hardware and infrastructure environments. Other standards shall be considered as preferred but not mandatory.

Scenario	Applicability of IT Standards
Software-as-a-Service (SaaS): PennDOT procures Software-as-a-Service from a vendor, and the solution is hosted in the vendor's environments or with a public cloud provider.	Low: The solution shall comply with the standards related to hosting requirements. All other standards shall be considered as preferred but not mandatory.

2.3 IT Standards Development

IT standards are not developed in response to a new IT project. Rather, they are developed through a collaborative process managed by PennDOT's Enterprise Architecture and Service Management (EASM) team. The IT standards development process includes participation from all levels of the organization, including: IT executives, technical managers, team leads, architects and hands-on developers and technicians. The effort includes a cross-section of the organization to bring differing technical expertise and perspectives, including infrastructure, applications, database, operations and security.

IT standards are proposed, documented, presented, discussed and deliberated in an objective and professional manner. This process is managed by the *EASM Workgroup*, which is made up of a select group of Division Chiefs and Section Chiefs from ISTO and also includes senior-level consultants. As needed, the EASM Workgroup reaches out into the organization to enlist hands-on technical experts to gather research and provide feedback on proposed standards and architecture decisions.

Draft standards are presented to the EASM Workgroup for concurrence. After EASM Workgroup consideration and approval, IT standards are presented to the EASM Program Governance Committee (PGC), consisting of PennDOT's IT Bureau Directors and the CIO. With EASM PGC approval, the proposed standards become official. Official IT standards are included in this document and distributed to the pertinent IT stakeholders within the organization.

2.4 Architecture Evaluation & Guidance

PennDOT will assign one or more enterprise architects to an IT project at the earliest point in the project lifecycle. The assigned architects specialize in infrastructure and application architecture, and they are familiar with PennDOT's Enterprise IT Standards. These architects will work with the business community and business analysts and with the projects technical and project management team to gather high-level functional and solution architecture requirements. The architects will then translate those requirements into the most optimal solution architectures.

Documents and deliverables produced by the enterprise architects may include:

- **Application Profile Questionnaire (APQ):** Collects the high-level functional and system requirements for new IT projects or solutions.
- **Solution Architecture:** Illustrates and describes the key elements of the technical architecture for a new IT solution, including the specification of *Enterprise Technologies*, *Enterprise Solutions*, infrastructure environments, system interfaces, etc.
- **Infrastructure Architecture Document (IAD):** Defines the logical infrastructure architecture for the IT solution, including servers, network connectivity, communication protocols, security, etc.

Enterprise architects will continue working with project teams throughout the project lifecycle to promote awareness of *Enterprise IT Standards* and to help ensure that the new solution architecture aligns with those standards while still meeting the needs of the business.

2.5 COTS and IT Standards

Commercial Off-The-Shelf (COTS) solutions can offer a significant cost savings and a reduced time-to-market when compared with a custom-developed IT solution.

If a COTS solution is to be hosted in PennDOT or Commonwealth environments and is to be supported in any way by PennDOT IT resources, then the COTS is bound by certain elements of our Enterprise IT Standards. As with any IT solution, a COTS solution must be evaluated for alignment with our Enterprise IT Standards. The time for this evaluation is *before* the COTS is selected and certainly before a purchase contract or some other type of binding commitment has been established. Implications of COTS solutions that don't align with Enterprise IT Standards and the potential for additional support costs must be weighed against any potential cost savings offered by the COTS.

COTS solutions are developed with a very specific set of technologies and with a target platform. While it may be technically possible to modify a COTS to bring it into closer alignment with our Enterprise IT Standards, caution must be taken, as these efforts are often very risky and may leave PennDOT with a solution that is orphaned by the COTS vendor and difficult to upgrade and maintain.

2.6 RFP/RFQ's and IT Standards

Any IT solution being proposed as part of a procurement (RFP, RFQ, etc.) is also bound by our Enterprise IT Standards. As part of the RFP/RFQ process, prospective vendors must complete a PennDOT *Offeror Technology List* showing all required technologies for their proposed solution and include this form with their technical proposal. Prospective vendors must also indicate how their proposed technical architecture aligns with our Enterprise IT Standards and weigh the costs and benefits of any non-alignment.

A careful architecture evaluation of the proposed IT solution shall be conducted and any non-alignment with Enterprise IT Standards shall be carefully documented and presented to key selection team members in advance of proposal scoring and vendor selection. **When evaluating potential vendor's proposed IT solutions, those that align with PennDOT *Enterprise IT Standards* are preferable to those that do not.**

2.7 Deviation from IT Standards

PennDOT recognizes that there may be strong business cases for IT solutions that deviate from our *Enterprise IT standards*. If a decision is made to proceed with an IT solution that does not align with our standards, a waiver request must be submitted and approved by PennDOT senior IT leadership. In some cases, in addition to approving the waiver, PennDOT's *Enterprise IT Standards* may be updated so future IT solutions can incorporate similar architectures.

The following six situations illustrate a deviation from these *Enterprise IT Standards*:

- **Violation of *Guiding Principles for Enterprise Architecture*:** This is a proposed architecture for an IT solution that is not in alignment with the *Guiding Principles for Enterprise Architecture* as identified in Section 3 of this document. Waiver required.
- **Violation of *Technical Architecture Guidelines*:** This is an IT solution that is inconsistent with one or more of the Technical Architecture Guidelines (TAG's) identified in Section 4 of this document. Waiver required.
- **Non-Standard Architecture:** This is the use of an architecture that is inconsistent with the standard *Reference Architectures* identified in Section 5 of this document. Waiver required.
- **Non-Use of *Enterprise Solution***: This is developing or acquiring new solution functionality that is the same or very similar to that which is already provided by a standard *Enterprise Solution* identified in Section 6 of this document. Waiver required.

- **Non-Use of *Shared Infrastructure***: This is deploying or using a new infrastructure environment that is the same or very similar to that which is already provided by a standard *Shared Infrastructure* identified in Section 7 of this document. Waiver required.
- **Use of Non-Standard Technology:** This is the use of any technology that is either not identified as an *Enterprise Technology* or that is prohibited for use in Section 8 of this document. Waiver required.

2.8 Information Technology Lifecycle Management

Information Technology Lifecycle Management (ITLM) is PennDOT's formal process to tracking technologies in use to support our business. The ITLM process helps the organization identify and respond to change brought about by the interaction of interdependent technologies and the movement of those technologies through their natural lifecycle from release and early adoption through obsolescence and retirement.

A key element of the ITLM process is the assignment of a lifecycle classification or status to all critical *Enterprise Technologies*. The Commonwealth of Pennsylvania, Office of Administration, Office of Information Technology (OA/OIT) has established a standard set of lifecycle classification system for all agencies to use.

The standard technology lifecycle classifications are as follows:

Classification	Description
Emerging	Emerging technologies or products that have the potential to become current standards. At the present time, they are to be used only in pilot or test environments where they can be evaluated. Use of these technologies is restricted to a limited production mode, and requires approval of a waiver request. Research technologies are less widely accepted and time will determine if they will become a standard.
Current	These technologies or products meet the requirements of the current architecture and are recommended for use.
Contain	These technologies or products no longer meet the requirements of the current architecture and are not recommended for use. They are to be phased out over time. No date has been set for their discontinuance.
Retire	These technologies or products are being phased out. Plans are to be developed for their replacement, especially if there is risk involved, such as lack of vendor support. A date for retirement has been set.

2.9 Application and Technology Inventory

PennDOT's applications and technologies represent critical IT assets that support our business. A single, comprehensive and up-to-date inventory is essential in order to effectively manage and rationalize these assets. To that end, PennDOT maintains the IT Asset Management system (ITAM). ITAM is a central database and a web portal that tracks our business applications, and technologies and the relationships between them. ITAM also identifies application and technology stakeholders. ITAM can be accessed at http://itam.pdot.state.pa.us.

ITAM supports the following processes that advance a sound IT ecosystem:

- IT Lifecycle Management (ITLM)
- Technology Refresh Planning
- Technology Impact Analysis
- Application Portfolio Management
- Legacy Modernization Planning
- Knowledge Maintenance and Transfer

- IT Skills Assessment

Keeping ITAM information up-to-date and accurate is critical to its usefulness. The ITLM process described above is used to ensure that the technology information is maintained. For our business applications, information is entered and maintained in ITAM as part of the IT project and Managed Maintenance processes.

3 STANDARD: Guiding Principles for Enterprise Architecture

3.1 Definition

A successful Enterprise Architecture program must be business-driven. Technical architecture must follow from the needs of the business. To ensure this business-centric approach, PennDOT's Enterprise Architecture and Service Management (EASM) program created a set of four *Guiding Principles for Enterprise Architecture* below. These principles define our EA strategy and govern all of our EA decisions, standards and processes from the top-down.

The remainder of this section defines PennDOT's standard *Guiding Principles for Enterprise Architecture*.

3.2 Guiding Principles for Enterprise Architecture

PennDOT's *Guiding Principles for Enterprise Architecture* are as follows:

- **Skills Availability:** The skills necessary to maintain and enhance our systems must be available now and 15 years into the future.
- **Security:** Data is protected from internal and external unauthorized access or disclosure.
- **System Agility:** Our technology must enable flexibility and scalability, resulting in quick and efficient response to new and emerging business needs, including legislative mandates.
- **Systematic, Iterative Change:** Change will be guided by systematic iterative road maps and agile project management strategies avoiding high risk "big bang" waterfall projects.

4 STANDARD: Technical Architecture Guidelines

4.1 Definition

There is a tremendous gap between the business-centric strategy defined by *Guiding Principles* and the day-to-day technical decisions needed to implement IT solutions. More precise technical guidance is needed to guide architects, developers and infrastructure administrators. To fill this gap between strategy and operational needs, PennDOT defines *Technical Architecture Guidelines* or TAG's. *Technical Architecture Guidelines* are set of technology-centric principles or precepts for IT architecture that guide the design of new IT solutions. To ensure business-centric EA and IT services, these *Technical Architecture Guidelines* must all align back to the *Guiding Principles*.

The remainder of this section defines PennDOT's *Technical Architecture Guidelines*.

4.2 General Technical Architecture

The following are PennDOT's Technical Architecture Guidelines for General Technical Architecture:

TAG#	Guideline Statement	Additional Explanation
ARCH.001	The solution shall comply with all Commonwealth standards defined by the Office of Administration/Office for Information Technology (OA/OIT) in Information Technology Policies (ITP's) and PennDOT IT standards as defined in this document.	Reaffirms the intent and the authority of OA/OIT standards and PennDOT's Enterprise IT Standards to effect a more standardized and optimal solution architecture.
ARCH.002	The solution shall comply with PennDOT's standard *Guiding Principles for Enterprise Architecture* to the greatest extent possible.	Encourages the review and evaluation of the new solution architecture against the standard *Guiding Principles for Enterprise Architecture* defined in Section 3 of this document.
ARCH.003	The solution shall comply with PennDOT's standard *Technical Architecture Guidelines* to the greatest extent possible.	Encourages the review and evaluation of the new solution architecture against the standard Technical *Architecture Guidelines* defined in Section 4 of this document.
ARCH.004	The solution shall align with PennDOT's standard *Reference Architectures* to the greatest extent possible.	Encourages the review and evaluation of the new solution architecture against the standard *Reference Architectures* defined in Section 5 of this document.
ARCH.005	The solution shall leverage PennDOT's standard *Enterprise Solutions* to the greatest extent possible.	Encourages the review and evaluation of the new solution architecture against the standard *Enterprise Solutions* as defined in Section 6 of this document.
ARCH.006	The solution shall leverage PennDOT's standard *Enterprise Infrastructure* to the greatest extent possible.	Encourages the review and evaluation of the new solution architecture against the standard *Enterprise Infrastructure* as defined in Section 7 of this document.

TAG#	Guideline Statement	Additional Explanation
ARCH.007	The solution shall leverage technologies in lifecycle classifications as defined by the Office of Administration/Office for Information Technology (OA/OIT) in Information Technology Policies (ITP's) and PennDOT IT standards as defined in this document as follows: • Only technologies with a lifecycle classification of "Current" or "Emerging" shall be used for new or significantly modified IT solutions. • Technologies with a lifecycle classification of "Contain" or "Retire" shall *not* be used for new solutions or introduced into existing solutions. • If no applicable OA/OIT or PennDOT policy defines a lifecycle classification for a technology, a waiver must be submitted if the technology is to be used.	This is intended to promote the use of current and emerging technologies while also encouraging the gradual reduction in the use of older technologies.
ARCH.008	The solution shall ideally be architected as a series of distinct and loosely-coupled horizontal tiers.	If possible, separate IT solutions into horizontal tiers, such as presentation, business, middleware, persistence, etc. Loosely-couple these tiers to allow for flexibility and change in the future.
ARCH.009	The solution shall ideally be architected as a collection of loosely-coupled vertical components based on the business functionality each component provides.	At the enterprise level, this vertical separation may mean separate focused yet integrated solutions for HR, Budget, Inventory, etc. Within a single solution, this may mean separate modules for functionality such as workflow, CRM, correspondence, administration/configuration, reporting, batch, etc. Loosely-couple these tiers to allow for flexibility and change in the future and perhaps for iterative delivery to the business customer.
ARCH.010	On-premises hosting is required for all IT solutions that manage confidential and/or PII data or are deemed mission-critical.	Applications that are mission-critical or that manage confidential data must be hosted in Commonwealth or PennDOT hosting facilities.

TAG#	Guideline Statement	Additional Explanation
ARCH.011	Public cloud hosting is appropriate for the following use cases: • Development, System and Performance Testing and Code & Configuration Management • Research and Innovation • Non mission-critical applications • Vendor-hosted and SaaS applications • Applications that do not manage confidential and/or PII data • Backup and Disaster Recovery • Public-facing and content-only sites	PennDOT has very little experience with public cloud. PennDOT and CWOPA decision-makers are not yet in a position to embrace public cloud in all use-cases, particularly where confidential and citizen data is concerned. It is recognized that public cloud, particularly PaaS and SaaS, can offer operational efficiencies provided the use-case is appropriate.
ARCH.012	For cloud-hosted solutions, Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) shall be considered before Infrastructure-as-a-Service (IaaS).	SaaS provides IT solutions to the business more quickly without the capital expenses for development or infrastructure. PaaS allows developers to deliver solutions without the capital and operating expenses of infrastructure. SaaS and PaaS allow infrastructure technicians to spend less time on hardware upgrades, OS and middleware patches and technology refreshes and spend more time in infrastructure design and optimization across the enterprise.
ARCH.013	The solution shall be scalable, with respect to infrastructure, technology and software architecture, to accommodate increases in system capacity and throughput without resulting in performance degradation.	Solution should run effectively in a clustered environment. Solution should respond well to horizontal and vertical scaling as demand for the solution grows.
ARCH.014	The solution shall encrypt sensitive data in motion and at rest as required in Commonwealth and PennDOT standards.	To protect confidential and PII data from unauthorized access.
ARCH.015	The solution shall be developed using Java EE or Microsoft C#.NET programming languages to the greatest extent possible.	Java and C#.NET are the two programming languages that PennDOT is best able to support for web applications and web services development.
ARCH.016	For solutions that primarily target desktop form factor devices, the solution shall be server-based to the greatest extent possible and be accessible with industry-leading web browsers.	Discourage the use of client-based applications (except for native mobile) and promote accessibility from multiple web browsers.

TAG#	Guideline Statement	Additional Explanation
ARCH.017	The solution shall be designed to be accessible via the internet unless there is a specific requirement to the contrary.	Promotes greater accessibility to enterprise applications for business users who are increasingly in the field or working from alternate locations.
ARCH.018	The solution shall have easily configurable parameters that do not require code modifications for such items as: communication, infrastructure and component names and locations, database names and connections, environment-specific settings, etc.	Configuration items that can change often should be easily changed with no coding changes and with minimal or no effort for deployment of these changes.
ARCH.019	The solution shall support multiple environments, including production and multiple pre-production environments.	Environments as needed for Sandbox, Development, System Test, UAT, Performance Test and Production.
ARCH.020	The solution shall include sufficient technical documentation, and implementation plans must incorporate specific tasks and activities to facilitate knowledge transfer and transition to designated PennDOT technical resources.	To ensure a smooth transition from the project development/build team to a steady-state maintenance/support team.

4.3 Commercial-Off-The-Shelf Software (COTS)

The following are PennDOT's Technical Architecture Guidelines for COTS solutions:

TAG#	Guideline Statement	Additional Explanation
COTS.001	The use of COTS middleware software is preferable to custom-development.	If there is a widely-used COTS technology to perform middleware functionality, it is most likely going to be more efficient to leverage that technology than custom coding in a general-purpose programming language like Java or C#.NET. Any efficiencies gained will have to be weighed against the cost of acquiring and supporting the COTS middleware technology.
COTS.002	The use of COTS business software is preferable to custom-development for providing business functionality that is common or non-unique to the organization.	Examples of such common business functionality include: HR, budget, service desk, etc. The more common the business function is, the better chance that a COTS is the way to go. COTS offering business functions that are common across a smaller number of organizations (e.g. 50 states or 67 counties) should be much more carefully evaluated for business fit before selection.

TAG#	Guideline Statement	Additional Explanation
COTS.003	The COTS software shall not be customized such that the organization is supported by a unique code base for the core product.	At this point, the solution would be considered custom development and should be managed as such.
COTS.004	The COTS software shall not be customized beyond 20% of the overall functionality.	As the level of customization increases, the advantages of the COTS vs. custom-development decreases. Beyond a certain level of customization, the COTS will be significantly more costly to develop, implement and maintain vs. custom-developed solutions.
COTS.005	The COTS software shall only be customized through configuration, configurable attributes, user exits, service interfaces or API integration with external solution components or services.	A leading issue with COTS is difficulty with upgrades and technology refreshes. Smart customization can substantially reduce the brittleness of the solution.
COTS.006	The COTS software must be recognized by independent technology-rating or industry groups as a leader for providing the intended functionality.	Recognition of COTS software by independent groups (e.g. Gartner, Forrester, etc.) or specific government or industry associations (e.g. AASHTO, AAMVA, etc.) can greatly reduce the risk associated with COTS.
COTS.007	The COTS software must be widely adopted in the industry or very likely to be adopted in the future.	The more customers there are for COTS software, the more likely the product will remain viable in the long term.
COTS.008	The financial and existential variability of the software vendor shall be carefully considered when evaluating COTS software.	COTS software can be in production for 10 years or more. The possibility that the software vendor could cease operations should be carefully considered.
COTS.009	The COTS shall be widely supported by the IT labor force or the required technical skills shall be readily attainable.	Skilled IT labor must be readily available or the skills must be easy to learn either on-the-job or through readily-available training.
COTS.010	The COTS software must include ongoing maintenance and support agreements with the software vendor so long as the COTS directly supports the business and/or is used in a production runtime environment.	The software vendor that develops the COTS must also offer maintenance and support agreements, and PennDOT must enter into these agreements to ensure the business is adequately protected. Maintenance and support agreements provide periodic fixes and enhancements as well as production support in the event of a defect or service interruption. Maintenance and support for COTS cannot be “turned over” to PennDOT resources, as this would then be a custom-developed solution.

TAG#	Guideline Statement	Additional Explanation
COTS.011	The cost of ongoing maintenance, COTS and technology upgrades and maintenance & support agreements must be considered when evaluating the costs of COTS software versus custom-development.	In addition to the upfront license costs, maintenance and support agreements cost typically range from 15% to 30% of the original license cost. These costs often increase each year based on some inflation index.
COTS.012	If a COTS business solution is offered as Software-as-a-Service (SaaS), the SaaS deployment model shall be considered before on-premises hosting, provided the use case is appropriate for cloud hosting.	Vendors can generally provide more efficient and cost-effective support for their COTS business solutions if they are offered as SaaS. The preference for SaaS does not apply for COTS middleware. Refer to TAG's regarding cloud hosting for the appropriate use cases.

4.4 Data Architecture & Management

The following are PennDOT's Technical Architecture Guidelines for Data Architecture & Management:

TAG#	Guideline Statement	Additional Explanation
DATA.001	Systems of record that must persist structured data for frequent querying or reporting shall do so using a relational database technology.	Even in an era of emerging technologies like no-SQL databases and Big Data, RDBMS are still the optimal choice for our transactional and operational systems of record.
DATA.002	Binary content, including: documents, images, videos, etc., shall be managed in a PennDOT-approved Content Management System and not in a relational database.	Documents/content shall be managed in a CMS, like EDMS (P8) or Microsoft SharePoint.
DATA.003	All confidential data, including: structured, unstructured and binary, shall be encrypted at rest.	Data must be encrypted at-rest and must only be accessible to authorized users.
DATA.004	All confidential data loaded, exported and exchanged among enterprise application databases shall be encrypted end-to-end.	Data must be encrypted in-transit and in intermediate resting locations.
DATA.005	Transactional (OLTP) and analytical (OLAP) data shall be managed in separate database environments, each being uniquely tuned for the required workloads.	Transactional databases must optimize transaction throughput and take extra measures to protect data integrity while analytical databases must optimize query performance. These disparate needs cannot efficiently be accommodated in a single environment.
DATA.006	The exchange of data in bulk to and from enterprise databases shall be through well-defined and documented interfaces.	Documented interfaces help in understanding dependency among enterprise applications and their databases.

TAG#	Guideline Statement	Additional Explanation
DATA.007	Applications shall not have direct query access to other applications' data.	Use ETL to move data from one application's database to another or use an EAI solution if real-time integration is a business requirement.
DATA.008	The use of COTS middleware tools for Extract, Transform and load (ETL) is preferable to custom coding.	COTS middleware is for more likely to deliver a better solution in less time and cost compared with custom coding. This is especially true for heterogeneous ETL (e.g. SQL Server to Oracle, ASCII text to Oracle).
DATA.009	Database code should not be used for routine CRUD operations; rather, dynamic SQL should be used instead.	Stored procedures can encapsulate business logic that may be best suited for the application tier, and they unnecessarily couple a frontend application to a specific database technology.
DATA.010	Database code should be reserved for long-running or highly-complex tasks involving data within a single database environment.	Database code (e.g. stored procedures, functions, etc.) is often the most performant option for such tasks but they should generally be avoided in all other cases.
DATA.011	Comprehensive, accurate and up-to-date data models shall be maintained for enterprise application databases using a COTS data modeling tool.	Ideally, this means logical and physical data modeling using the modeling tool, including the generation of DDL scripts for model-driven database development. At minimum, data models should be refreshed with each significant database change.
DATA.012	Databases for all enterprise applications shall be designed by a specially-trained and experienced data modeler.	Data modeling should not be left to individual developers except for the smallest of changes (e.g. adding or modifying the definition of a single column). An experience data modeler should take ownership and be responsible for the database design.
DATA.013	Technical and business definition metadata for all enterprise application databases shall be loaded to the enterprise metadata repository and refreshed on a regular bases.	The metadata repository makes metadata easy to search, explore and analyze by developers, DBA's, BA's and even the business user.
DATA.014	The solution shall document and implement an Information Lifecycle Management (ILM) strategy, including record retention and archiving/purge strategies, for all structured and unstructured data.	Promote sound ILM and efficient utilization of storage as well as maintain optimal query performance of mainline production transactional processing.

4.5 Enterprise Application Integration

The following are PennDOT's Technical Architecture Guidelines for Enterprise Application Integration (EAI):

TAG#	Guideline Statement	Additional Explanation
EAI.001	A single enterprise inventory of all EAI services and interfaces shall be developed and kept current.	This is critical to understanding applications' dependencies upon one another, for application and data governance and for analyzing the impact of change on applications.
EAI.002	All EAI services and interfaces must be secured with Authentication and Authorization of the service consumer in a manner consistent with OA/OIT policies.	This means Authentication and Authorization against the appropriate Commonwealth enterprise Active Directory.
EAI.003	All EAI services and interfaces shall be designed for security with the assumption that PennDOT and Commonwealth networks and IT environments are no more secure than the Internet.	The notion that a secure perimeter exists that insulates internal environments from security threats is no longer valid.
EAI.004	All confidential data exchanged via EAI services and interfaces must be encrypted in transit and at rest from end-to-end.	To protect confidential and PII data from unauthorized access.
EAI.005	EAI services and interfaces are the preferred architecture pattern to be used to satisfy business requirements for real-time access to data and services among systems.	Planned, designed, documented and managed SOA interfaces over firewall-friendly and easily-secured HTTP/HTTPS are far better than unrestricted direct query access.
EAI.006	EAI services and interfaces are only to be implemented when real-time or near real-time, access to data and services among systems is a business requirement; if not, a data integration approach should be used.	SOA services are preferable for real-time; however, if latency (e.g. hourly, daily, etc.) is acceptable, data integration solutions (e.g. ETL) are easier to implement and maintain, less tightly-coupled and more resilient.
EAI.007	The use of middleware for delivery of EAI solutions is preferable to writing custom application code.	Middleware generally results in better solutions that are built in less time, lower cost and with greater quality.
EAI.008	Existing middleware tools should be considered first for delivering EAI solutions.	
EAI.009	A balanced, proactive and reactive approach shall be taken to evaluate EAI tools against changing technology and business needs, and additional tools will be considered, evaluated and adopted through a formal change management process governed by the EASM program.	Proactive approach based on changing and emerging technologies and business needs. Reactive approach that responds to specific IT solution needs that cannot be addressed with existing tools.
EAI.010	Common EAI Patterns shall be developed that define how middleware and other common architectural components will be used, and these patterns shall be considered first for delivery of EAI solutions.	Identify the smallest number of pre-defined, preferred architectural patterns to optimally address known and expected EAI use cases, and encourage their use on IT projects.
EAI.011	A balanced, proactive and reactive approach shall be taken to evaluate EAI Patterns against current and emerging EAI Use Cases, and new patterns shall be developed in a formal change management process that is managed by the EASM program.	Proactive by considering changing and emerging use cases. Reactive in response to specific IT solution needs that cannot be addressed with existing patterns.

TAG#	Guideline Statement	Additional Explanation
EAI.012	EAI mediation functionality and components should be confined to middleware tools and environments to the greatest extent possible.	Mediation (security, translation, transformation, etc.) should take place in middleware environments.
EAI.013	Applications and application environments should be kept free from EAI mediation functionality and components to the greatest extent possible.	Applications and their environments should be free from mediation and middleware components, plugins, adaptors, etc.
EAI.014	EAI services and interfaces should use broadly-recognized standards, protocols and conventions when they are available.	Use of HTTP/HTTPS, SOAP, REST, XML and JSON for message format, and industry standards like CMIS for message content.
EAI.015	SOAP web services are the preferred architecture for EAI as more of the following conditions are met: • The service is a Common Service, • A formal or contractual relationship exists between the service provider and the service consumer, • The service has a small number of well-defined consumers, • There is a need for standards-based security from end-to-end, • The service provider and service consumer are both enterprise application, • The service is coarse-grained and expected to evolve more slowly over time. • The service provider and service consumer need to be insulated from change. • The message payload has a large amount of complex business data and validation requirements, and • The message payload contains documents or other large binary attachments.	Generally, SOAP is the preferable (but certainly not exclusive) architecture for Common Services at the center of the enterprise or for services extended formally to our known/managed business partners.

TAG#	Guideline Statement	Additional Explanation
EAI.016	REST web services are the preferred architecture for EAI as more of the following conditions are met: • The service is a Solution-Specific Service, • The service consumers are primarily mobile or mobile web client applications, • There are bandwidth and client performance constraints • The service is fine-grained or specific to a narrow business function or transaction, • There are a very large number of consumers that are less well-known • The service API and/or the consuming application need to evolve rapidly and share in that rapid change, • There is a large volume of service requests that benefit from caching and other native benefits of REST.	Generally, REST web services are the preferred (but certainly not exclusive) architecture for rapidly-evolving, high-volume, fine-grained services that typically exist at the perimeter of the enterprise, for example in a Web API for public-facing mobile or web clients.
EAI.017	All Common Services shall be planned, designed, developed, managed and governed by a formally-recognized team.	
EAI.018	All Common Services should incorporate monitoring, logging and instrumentation for availability, utilization, responsiveness and adoption to facilitate Service Management.	Collect, store and present data on request transaction volume, response time, number of consumers and other metrics to facilitate Service Management
EAI.019	A Service Wrapper shall be implemented as a Common Service around COTS API's to better govern consumer access to COTS functionality and to insulate consumers from complexity and change.	Service wrapper will simplify consuming of COTS service API's (e.g. FileNet P8) and ease transition to another COTS in the future.
EAI.020	Solution-Specific Services are to be used only for specialized integration requirements between a provider and a small number of consumers, where broad reuse is not an anticipated requirement.	Mandating Common Services for all services will create bottlenecks, increase costs and time-to-market.

4.6 Identity & Access Management

The following are PennDOT's Technical Architecture Guidelines for Identity & Access Management:

TAG#	Guideline Statement	Additional Explanation
IAM.001	All enterprise applications shall leverage Commonwealth enterprise employee, business partner and citizen directories for managing user identities and credentials.	This means Microsoft Active Directories CWOPA (employee/internal consultant), Managed_Apps (business partner) and SR_PROD (citizen).

TAG#	Guideline Statement	Additional Explanation
IAM.002	All enterprise applications and services accessible beyond PennDOT's network environments shall leverage Commonwealth and PennDOT standard access management technologies for authentication, coarse-grained authorization and auditing.	Currently, this includes CA products, such as: SiteMinder/Single Sign-On, IdentityMinder/Identity Manager and Secure Proxy Server/Access Gateway. Also includes IBM DataPower for web services. Coarse-grained means at the site or folder level or at most granular, the web page level.
IAM.003	Commonwealth enterprise directories are the preferred location for managing common user roles and attributes.	If user roles and attributes are managed in AD along with core user data, it is easier promote reuse and to deliver Identity Management and user provisioning solutions.
IAM.004	All enterprise applications shall implement a fine-grained authorization and access management architecture that is externalized from application code and that follows broadly-recognized industry patterns.	Manage configurable data in directories, external files and/or database tables. Implement using patterns like RBAC, ABAC and/or CBAC.
IAM.005	Users of enterprise applications and services shall have the ability to perform Identity Management transactions in self-service fashion to the greatest extent possible.	This includes such Identity Management transactions as initial account creation, account update, password reset/forgot password, etc.
IAM.006	User administration and provisioning of application entitlements shall be delegated to business owners and external business partners to the greatest extent possible.	Delegated administration allows business the flexibility to provision applications they own, and allowing business partners to administer their own users saves Department resources.
IAM.007	The use of widely-available COTS technologies to deliver IAM functionality is preferable to custom coded solutions.	Use of technologies like CA suite, Microsoft Active Directory, etc.
IAM.008	All enterprise applications and services shall be accessible over the Internet unless there is a compelling business need to the contrary.	Think Internet first in order to maximize our capability to offer services to business partners and the public and to support increased accessibility and mobility for our employees.
IAM.009	All enterprise applications and services shall support Single Sign-On to the greatest extent possible.	When logged into PennDOT network, users should not be challenged for login when accessing enterprise applications. When accessing via the Internet, users should only be challenged once when accessing many enterprise applications.

5 STANDARD: Reference Architectures

5.1 Definition

A *Reference Architecture* combines *Enterprise Technologies* and *Enterprise Solutions* in order to define the highest-level logical architecture to support the critical capabilities and services needed to deliver IT solutions. An enterprise *Reference Architecture* defines the architecture for the entire IT environment for an organization. In addition to the enterprise *Reference Architecture*, large, complex organizations like PennDOT often need to define several more focused *Reference Architecture Perspectives* with each one covering a functional area, such as Identity & Access Management (IAM) or Data Warehousing and Business Intelligence (DW/BI).

The solution architecture for a particular business IT solution will draw from one or more of the *Reference Architecture Perspectives*. New IT solutions being designed will be directed towards incorporating existing *Reference Architecture Perspectives* to the greatest extent possible. This reduces design effort, time and cost while also ensuring that existing technologies, solutions and physical infrastructures are rationalized and standardized.

The remainder of this section defines PennDOT's standard *Reference Architecture and Perspectives*.

5.2 Present vs. Future State Reference Architecture

As an organization's business needs and strategy change, IT must respond and change the Reference Architecture as needed to meet the changing needs. In large organizations, change is constant, and it can be difficult to depict an exact Reference Architecture. Additionally, Reference Architecture is used for solution and project planning that can have long lifecycles, and a future perspective may be more relevant than the precise present-state.

The Reference Architecture depicted in Figure 2 and the various Perspectives in the remainder of this section attempt to strike a balance between present and future state that will have the broadest usefulness to many audiences. Where appropriate, the Reference Architecture Overview section calls out future plans that may be relevant. In addition, the Reference Architecture diagram has a Future Considerations section to illustrate totally new technologies that may be introduced to PennDOT's enterprise IT landscape in the next two years.

The most significant change coming to PennDOT's IT architecture is the gradual movement away from IFL/zLinux and x86/Microsoft Windows to x86/Linux for web, application, database and middleware platform hosting. Additionally, technology refreshes are always in process, including: FileNet Panagon to P8 and WebSphere Message Broker to IIB.

IT architects should work with PennDOT's EASM architects to address any questions they may have regarding the present and future-state Reference Architecture and how pending changes may impact their solutions or projects.

5.3 Enterprise Reference Architecture - Diagram

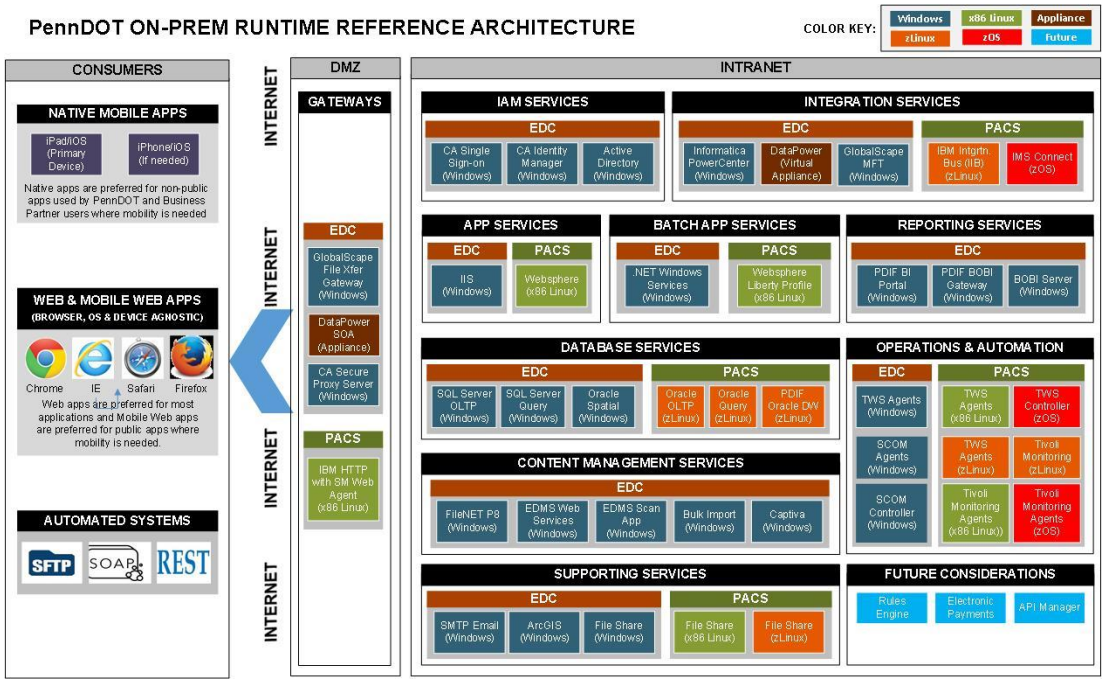

Figure 2: Enterprise Reference Architecture – Conceptual

5.4 Enterprise Reference Architecture - Overview

5.4.1 Consumer Components

Consumer components represent, from a technical perspective, the types of external consumers that interact with PennDOT applications and services, including:

1. **Native Mobile Apps:** Native mobile applications are developed only for non-public-facing applications that are used by PennDOT employees and business partners. Example use cases include: Road and Bridge Inspections or Driver Licensing Skills Test Exams. These applications are primarily developed for the Apple iOS platform and iPad device. Other platforms and devices are as needed.
2. **Web & Mobile Web Apps:** Browser-based web applications, including Mobile Web, are the predominant architecture for applications that are used by PennDOT employees, business partners and the general public. These applications are agnostic to the client device, OS and browser to the extent practical, and they are mobile accessible or mobile-friendly as business needs require.
3. **Automated Systems:** Interfaces between automated external systems and PennDOT applications and services shall be implemented with SFTP, REST and SOAP web services.

5.4.2 DMZ/Gateway Components

DMZ/Gateway Components are the solution components that reside in the DMZ and provide external consumers secure access to PennDOT's applications, services and file transfer resources, including:

1. **IBM HTTP Server w/ CA SiteMinder Agent:** PennDOT uses IBM HTTP Server (IHS) with CA SiteMinder Agents to provide Authentication, Authorization and Audit (AAA) as well as web content serving and reverse-proxy services to support our web applications.

   Note: The ESEC project will deliver a centralized web application gateway built around CA Secure Access Gateway that will replace the distributed agent architecture; however, the agents are the standard architecture at this time.

2. **CA Secure Proxy Server:** PennDOT uses CA products for Identity and Access Management (IAM), including Secure Proxy Server (SPS). SPS is hosted at EDC in Harrisburg and provides Access Management primarily for Microsoft .NET applications that require Internet accessibility.

   Note: The ESEC project will implement a newer version of CA access management technology called Secure Access Gateway which will be used for applications built with Java EE and Microsoft .NET as well as other technologies.

3. **IBM DataPower Appliance:** The IBM DataPower XI52 appliance, hosted at EDC in Harrisburg, provides Authentication, Authorization and Audit (AAA), reverse proxy and perimeter integration services (e.g. protocol conversion, XML mapping, message transformation, etc.).
4. **GlobalScape MFT:** PennDOT leverages the GlobalScape Managed File Transfer (MFT) product to provide SFTP file exchange with external systems.

5.4.3 Intranet Components

Intranet Components are PennDOT's internal solution components that are the core of our enterprise architecture and support our applications and services. These components are hosted at EDC in Harrisburg and at PACS in Ashburn, Virginia.

5.4.3.1 Identity & Access Management

Identity & Access Management (IAM) Services refers to our core IAM solution components which are hosted at EDC in Harrisburg. These components work in tandem with our Gateway components (e.g. CA SiteMinder Agents and SPS) to provide secure access to PennDOT applications and services, including:

1. **CA Single Sign-On:** Formerly called CA SiteMinder, this includes the Policy Server and administration UI that support runtime authentication and authorization as well as policy configuration and authoring. CA Single Sign-On is hosted at the EDC in Harrisburg.
2. **CA Identity Manager:** Formerly called CA IdentityMinder, this is the CA IAM component that provides a UI that supports user administration, delegated administration, provisioning and user self-service transactions. CA Identity Manager is hosted at the EDC in Harrisburg.
3. **Microsoft Active Directory:** The Commonwealth of PA has established three enterprise Active Directories for employees (CWOPA), business partners (Managed Apps) and citizens (SR Prod). PennDOT applications must use these directories to store user, credential, group and application entitlement information. AD infrastructure is hosted at the EDC in Harrisburg.

   Note: Some applications also manage application entitlements (roles, user attributes, etc.) used for fine-grained authorization in their own relational databases.

5.4.3.2 Integration Services

Integration Services defines the middleware technologies, hosted at EDC in Harrisburg and PACS in Ashburn, Virginia, that provide application, data and file integration services, including:

1. **Informatica PowerCenter:** Informatica PowerCenter is hosted at EDC in Harrisburg and provides data integration and Extract, Transform and Load (ETL) services to, from and among PennDOT enterprise application data stores as well as from transactional data sources to the PDIF Data Warehouse.
2. **IBM Integration Bus (IIB):** Formerly called WebSphere Message Broker (WMB), IIB is PennDOT's standard Enterprise Service Bus (ESB) middleware technology. It is hosted at PACS in Ashburn, Virginia and provides enterprise application integration services to, from and among PennDOT's enterprise application systems.
3. **IBM DataPower Virtual Appliance:** This is a virtual appliance version of the IBM DataPower that is used in our DMZ as a web service gateway. In our Intranet and hosted at EDC in Harrisburg, this IBM DataPower virtual appliance provides web services security, reverse proxy and lightweight EAI services (e.g. protocol and message format translation services, XML mapping, etc.) to, from and among PennDOT's enterprise applications.
4. **GlobalScape MFT:** GlobalScape MFT is hosted at EDC in Harrisburg and provides secure file transfer services to, from and among PennDOT's enterprise applications. GlobalScape also sits in DMZ to provide file transfer services to and from external consumer applications and PennDOT applications.
5. **IMS Connect:** IMS Connect is hosted in the z/OS mainframe environment at PACS in Ashburn, Virginia and provides TCP/IP gateway access to IMS transactions to facilitate legacy application integration. IMS Connect is used most commonly in conjunction with IBM Integration Bus (IIB) to provide IMS transactions as web services for easier integration of legacy applications with modern applications.

5.4.3.3 Application Services

Application Services refers to the solution components hosted at EDC in Harrisburg and at PACS in Ashburn, Virginia that provide application services for Java EE and Microsoft .NET applications and web services, including:

1. **IBM WebSphere Application Server:** WebSphere Application Server (WAS) is hosted at PACS and provides Java EE application services. WAS and Java EE are PennDOT's preferred architecture for our custom-developed mission-critical applications.

2. **Microsoft Internet Information Services:** Internet Information Services (IIS) is hosted at EDC in Harrisburg and provides application hosting services for .NET web applications and web services. Although Java EE and WAS are the preferred architecture for our in-house, custom-developed applications, we also have a sizeable footprint in the .Net/IIS architecture. IIS supports some custom-developed and COTS applications, including: PDIF BI Portal, dotGrants, eCAMMS & Lab applications and dozens of others.

5.4.3.4 Batch Application Services

Batch Application Services refers to solution components hosted at both EDC and PACS that provide batch or non-real-time application execution services where these services must be custom-developed in either Java EE or Microsoft .NET, including:

1. **WebSphere Liberty Profile:** IBM WebSphere Application Services (WAS) Liberty Profile is a streamlined implementation of WAS that PennDOT has hosted in PACS to provide an enterprise Java EE batch execution environment for custom-developed solutions.
2. **.NET Windows Services:** For .NET applications hosted at EDC, PennDOT recommends developing Windows Services in C#.NET to address any custom batch application needs.

5.4.3.5 Content Management Services

Content Management Services refers to the solution components, hosted at EDC in Harrisburg, that provide enterprise document, image and content management services, including capture, storage, indexing, searching, retrieval, archiving, etc. These components are collectively referred to as Electronic Document Management System (EDMS). The modernized P8-based solution will be renamed Enterprise Content Services (ECS). These components include:

1. **IBM FileNet P8:** FileNet is hosted at EDC in Microsoft Windows environment. FileNet is the core document and content management repository for the enterprise.

   > **Note:** PennDOT is currently in the process of implementing FileNet P8 as a modern replacement for our FileNet Panagon repository. Currently, new IT solutions are being directed to use the new P8 environments while existing solutions will be migrated from Panagon to P8 over the coming 18 to 24 months.

2. **EDMS Web Services:** Refers to the SOAP-based web services components that act as wrapper services around FileNet. These services are hosted at EDC in Harrisburg and are used by line-of-business applications to integrate seamlessly with FileNet. These web services are provided for both the legacy FileNet Panagon repository as well as the new P8 repository.
3. **EDMS Scan Application:** EDMS Scan application is a custom-developed web application that provides a highly-configurable image scanning solution. This application, hosted at EDC in Harrisburg, allows user to scan and index documents and send those documents to the FileNet repository.
4. **Bulk Import:** EDMS provides solutions for high-speed ingestion of documents and index data into the FileNet repository. Solutions are hosted in EDC and provide bulk import services for both the legacy Panagon and new P8 repositories.
5. **EMC Captiva:** EMC Captiva provides image capturing and image processing services, such as OCR and hardcode recognition. Captiva is used in conjunction with high-speed scanners, primarily by Driver and Vehicle Services (DVS).

5.4.3.6 Database Services

Database Services refers to solution components hosted at both EDC and PACS that provide enterprise grade data management for structured data, including:

1. **SQL Server (OLTP):** Located at EDC, these are Microsoft SQL Server databases that are configured to support optimal online transactions processing (OLTP). This is the default choice for PennDOT .NET applications because of skills alignment with .NET development/maintenance teams and cloud-readiness on Azure.
2. **SQL Server (Query):** Located at EDC, these Microsoft SQL Server databases support reporting and other read-only functions. The goal is to offload report processing (especially those that involve expensive, long-running queries) to the query databases and use the OLTP databases primarily for transaction processing. For all PennDOT applications that use SQL Server for OLTP, a corresponding SQL Server Query database is created. This query database is typically a mirror image of the OLTP counterpart and is synched with the OLTP database on a nightly basis using native SQL Server replication. More frequent synching with the OLTP database is possible on a case-by-case basis based on business needs.
3. **Oracle (Spatial):** Primary repository of PennDOT's geospatial data, this Oracle database is located at EDC. Most of the non-spatial data in the database are attributes extracted from various PennDOT systems that are necessary to support the data layers to display custom data on maps. Applications that have tightly-coupled geospatial functionality also use the database to store application OLTP data.
4. **Oracle (OLTP):** Currently on zLinux, these Oracle databases are hosted at PACS. Oracle is the default choice for PennDOT Java applications.
5. **Oracle (Query):** Similar to SQL Server Query databases, these Oracle databases are day old, read-only databases primarily for reporting purposes. Like its OLTP counterpart, these are on zLinux at PACS.
6. **Oracle (DW/BI):** Hosted on zLinux at PACS this database is PennDOT enterprise Data Warehouse. It supports operational reporting and data analytics, especially cross-system reporting and dimensional analysis. It consists of many schemas to support various functions, including: Staging, Operational Data Store (ODS), data marts for On-Line Analytical Procesing (OLAP) and a metadata repository.

5.4.3.7 Operations and Automation

Operations and Automation includes the solution components that support cross-platform orchestration of jobs and monitoring of infrastructure and application events, including:

1. **TWS (Tivoli Workload Scheduler):** Schedules, executes and tracks jobs on multiple platforms. At PennDOT, the Controller runs on zOS at PACS and programs known as tracker-agents run on machines under its control, both at PACS and EDC. Using the tracker-agents, TWS can orchestrate jobs across all supported platforms: zOS, zLinux, x86 Linux and Windows.
2. **Tivoli Monitoring:** With the Controller running on zLinux at PACS, Tivoli can be configured to monitor events on zLinux, zOS and x86 Linux. Currently, Windows machines are not monitored by Tivoli.
3. **SCOM (System Center Operations Manager):** SCOM is used to monitor Windows machines. The Controller runs on Windows at EDC and can be configured to monitor other Windows machines that run SCOM agents.

5.4.3.8 Supporting Services

Supporting Services are additional services that are commonly used by PennDOT applications, including:

1. **SMTP:** Located on Windows at EDC, PennDOT SMTP servers work with the OA SMTP servers to send out emails from on premise applications.

2. **ArcGIS:** ESRI's ArcGIS provides stand-alone map based applications as well as geo spatial services that can be used by any application to integrate map-based functionality within its native user interface.
3. **File Share:** Many applications and products use file shares as a common location to *share* files with different components of the same application or across application boundaries. File shares can be on the same or different operating system as the application using the file share.

5.4.3.9 Future Considerations

Future Considerations include technologies that may become a part of future-state Reference Architecture at PennDOT. Included here are only those components that are expected to have a significant impact on the design or operation of applications within the next 2 years, including:

1. **Business Rules Management System:** A Business Rules Management System (BRMS) provides tools to author and manage business rules and includes a business rules engine (BRE) to execute the rules at runtime. While enterprise class rules engine usually run as processes separate from the applications invoking them, some BRMS solutions provide options to embed the rules engine within applications. A BRMS solution may be helpful for implementing complex business rules when modernizing Driver and Vehicle Services (DVS) applications.
2. **Electronic Payments:** PennDOT would like to have a full range of consistent electronic payment options for both online and in-person transactions. While detail business requirements will drive the implementation details, support for credit cards and PCI (Payment Card Industry) compliance is a key requirement.
3. **API Manager:** Provides a solution for defining and managing APIs (Application Programming Interfaces) for internal use and external consumption. Usually the interfaces are in the form of SOAP and RESTful web services. API Manager can produce analytics on API usage and socialize APIs in a portal, for both internal and external stakeholders. IBM's API Manager can be configured to deploy and monitor services on DataPower, PennDOT's SOA Gateway.

5.5 BI and Reporting Perspective

Below is a logical illustration of PennDOT's standard BI and Reporting Reference Architecture.

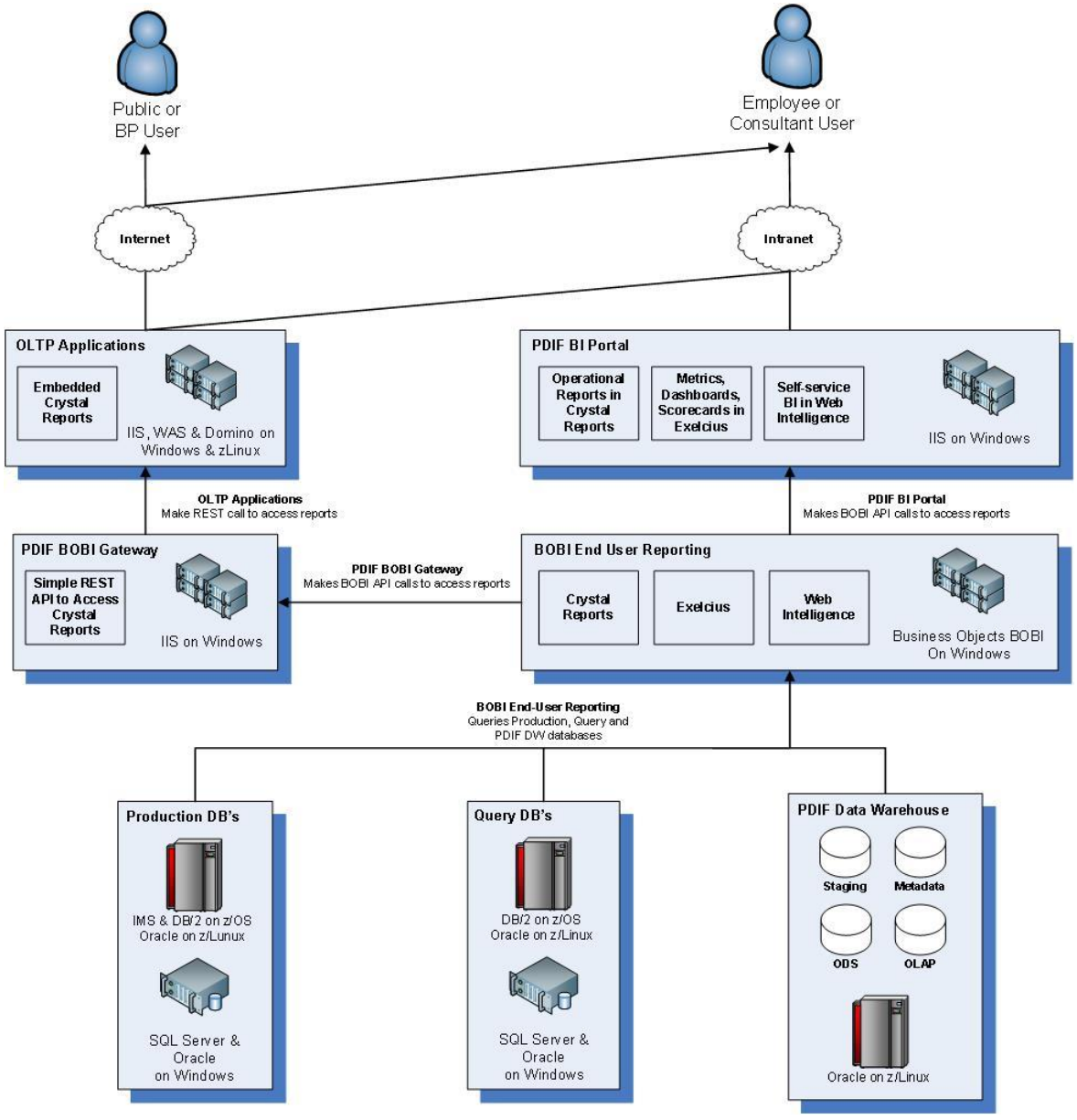

Figure 3: BI and Reporting Reference Architecture Perspective

5.6 Data Integration Perspective

Below is a logical illustration of PennDOT's standard Data Integration Reference Architecture.

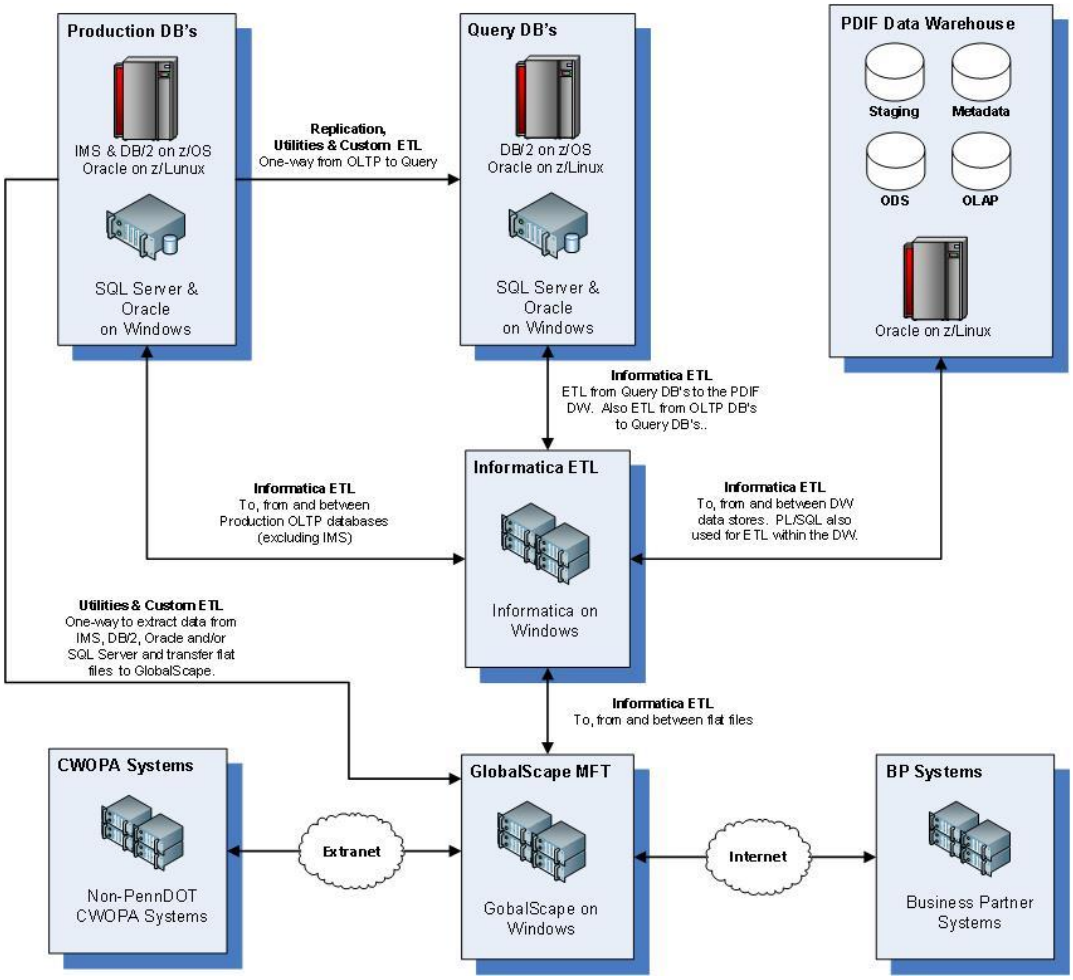

Figure 4: Data Integration Reference Architecture Perspective

5.7 Enterprise Application Integration Perspective

Below is a logical illustration of PennDOT's standard EAI Reference Architecture.

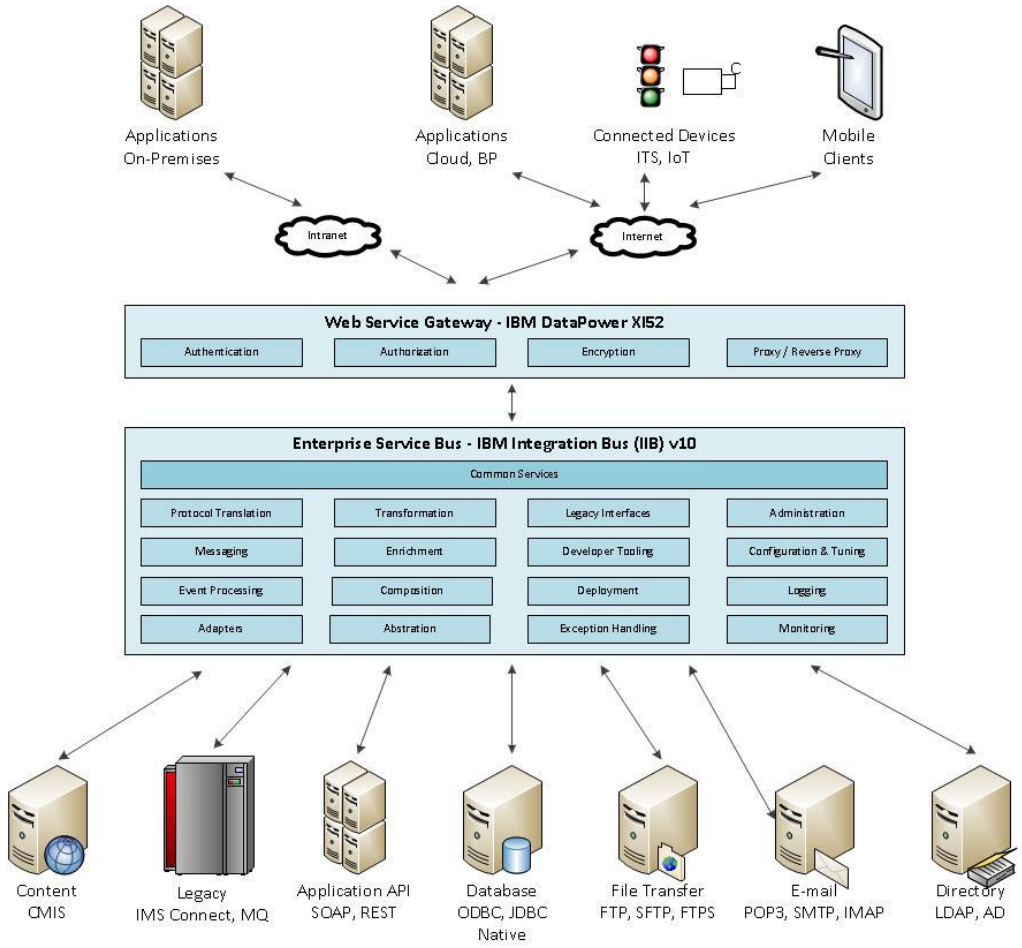

Figure 5: EAI Reference Architecture Perspective

5.8 Mobile Applications Perspective

Architecture Reference for Mobile Applications

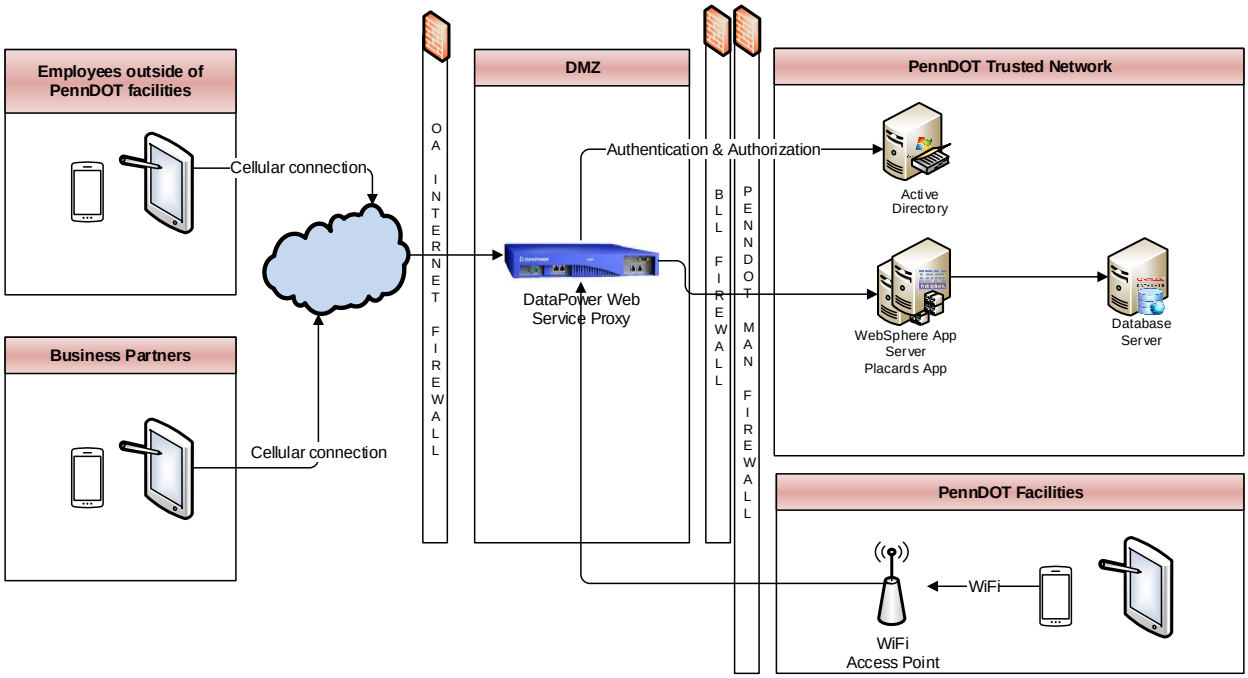

Figure 6: Mobile Applications Reference Architecture Perspective

5.9 Identity and Access Management Perspective

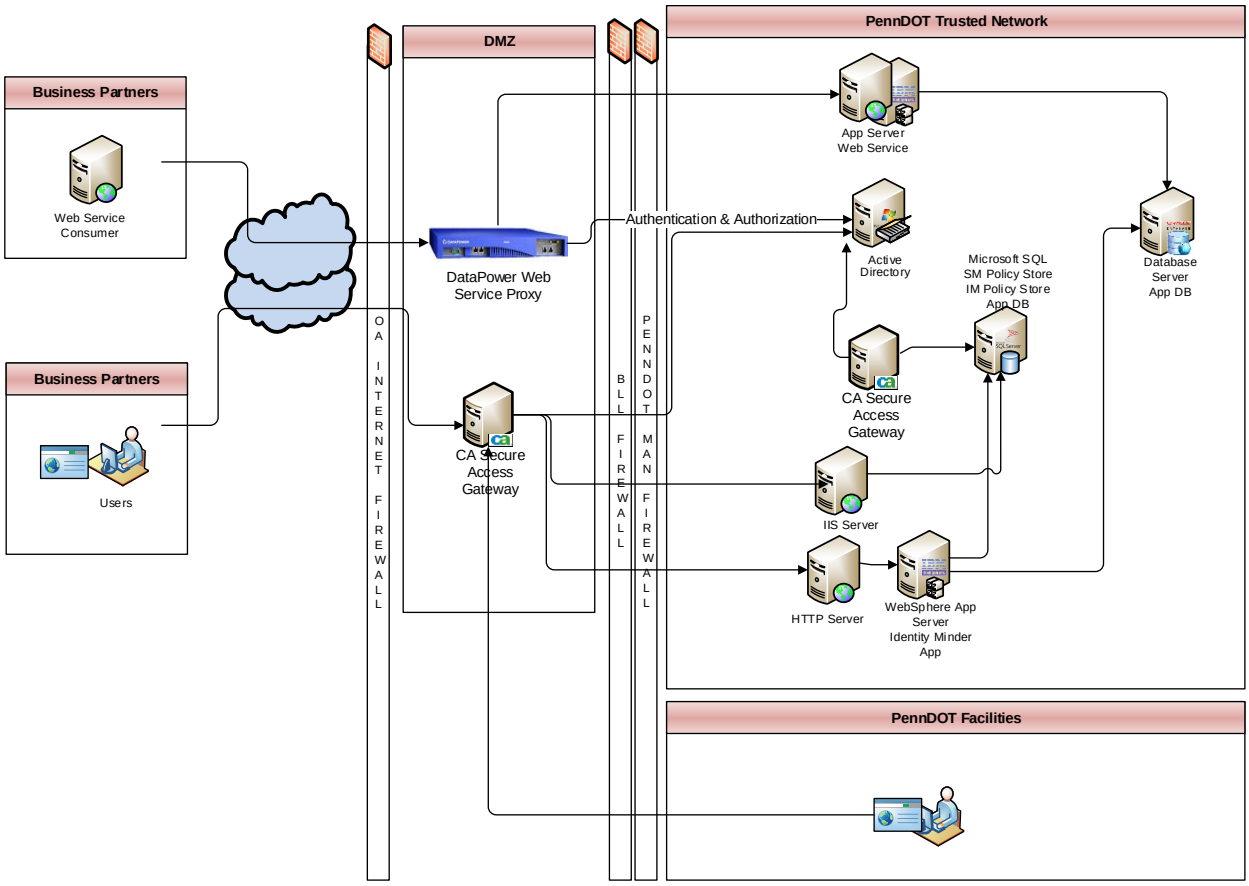

Figure 7: Identity and Access Management (IAM) Reference Architecture Perspective

5.10 Automation & Orchestration Perspective

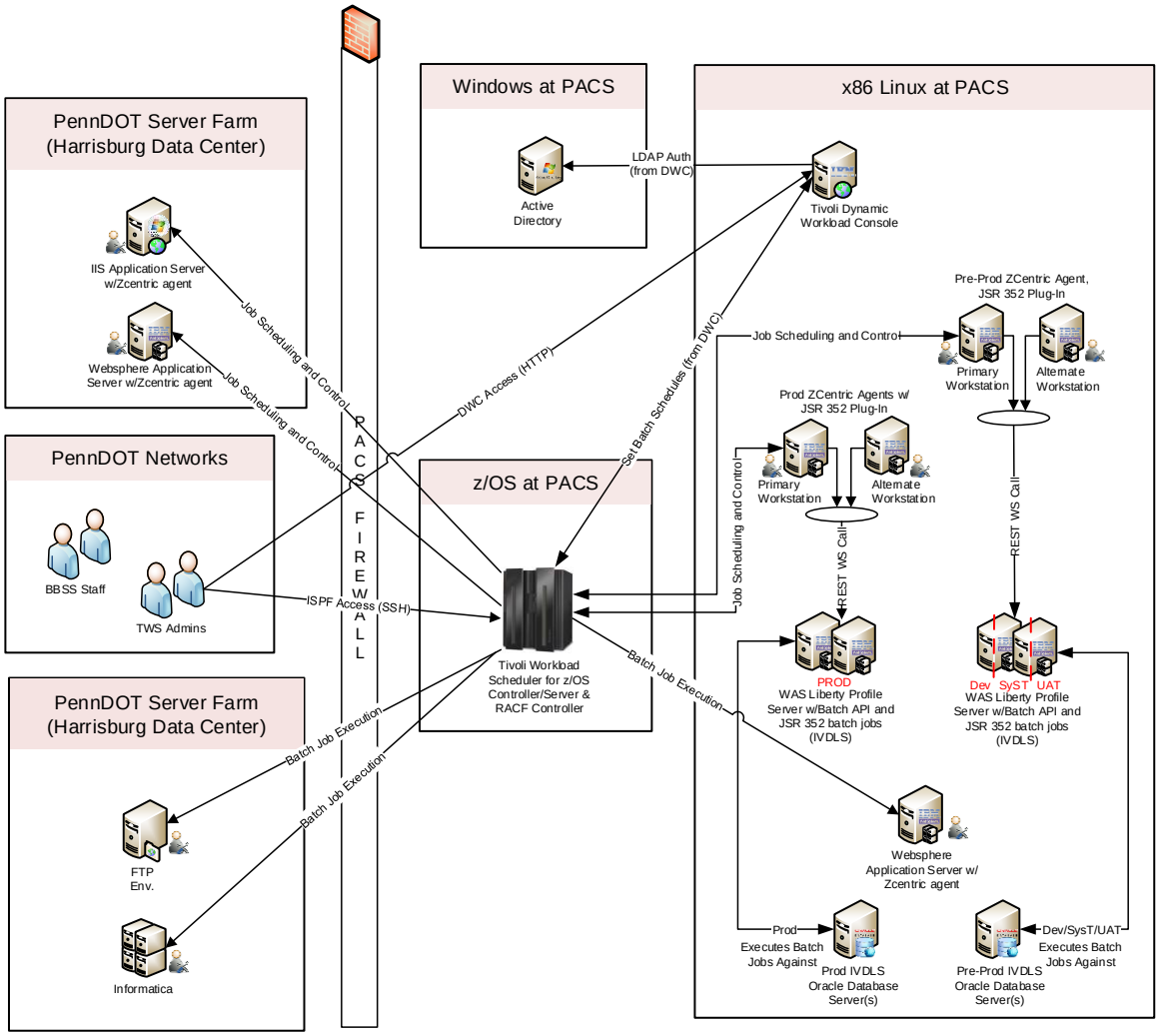

Figure 8: Automation and Orchestration Reference Architecture Perspective

5.11 Enterprise Content Services Perspective

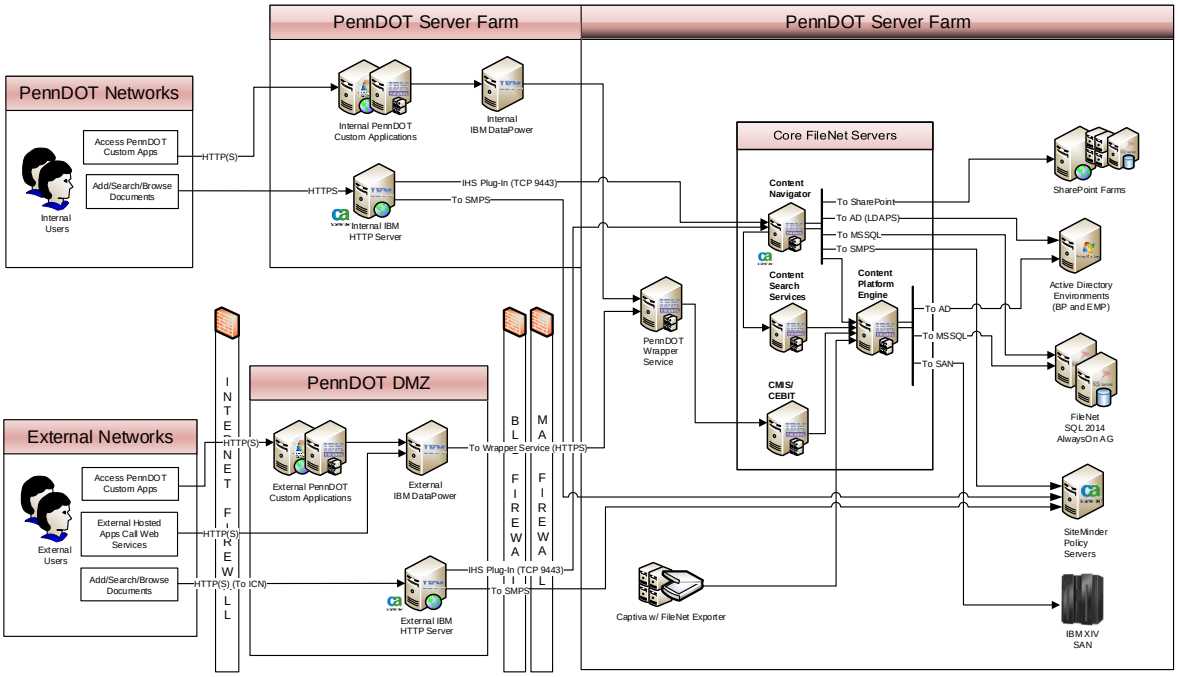

Figure 9: Enterprise Content Services Reference Architecture Perspective

5.12 System Monitoring Perspective

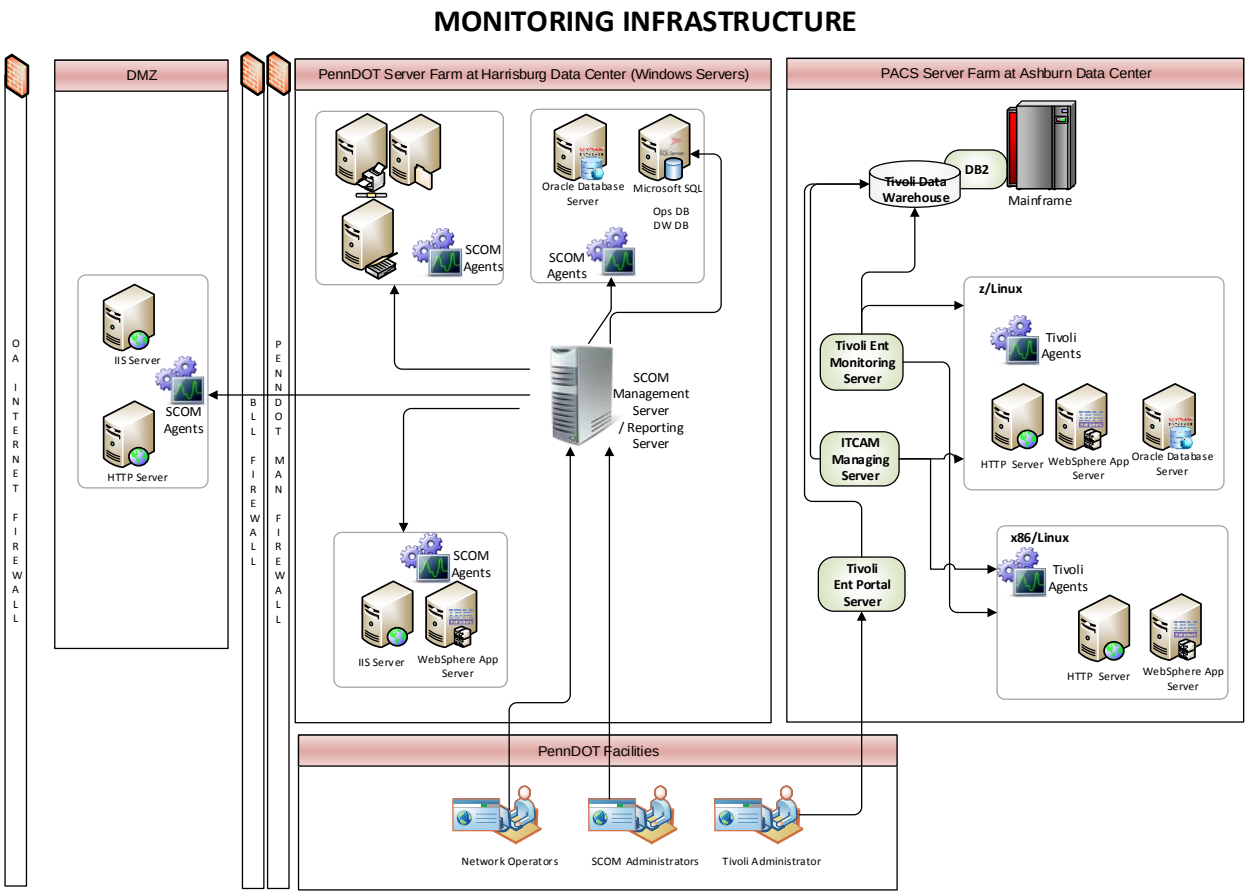

Figure 10: System Monitoring Reference Architecture Perspective

6 STANDARD: Enterprise Solutions

6.1 Definition

Enterprise Solutions are enterprise IT assets (e.g. applications, web services, frameworks, etc.) which provide a common set of functionality that is made available to be leveraged by many PennDOT IT solutions. *Enterprise Solutions* benefit the organization in that resources are not wasted developing more than a single solution with the same or nearly identical functionality. Some examples of *Enterprise Solutions* at PennDOT include: Electronic Document Management System (EDMS) for content management, PennDOT Java Framework (PDJF) for Java web applications development and PennDOT Data Integration Facility (PDIF) as the web portal for operational and analytical reporting solutions.

The remainder of this section defines PennDOT's standard *Enterprise Solutions.*

6.2 Enterprise Solutions

Solution	Description
Address Verification Service	This is a SOAP web service that provides postal address verification and standardization services. It acts as a wrapper service around the Finalist COTS package.
EDMS Bulk Import	EDMS provides a bulk import solution for high-speed mass ingestion of content and index information into the IBM FileNet repository,
EDMS Captiva	EDMS provides a Captiva solution that support OCR and other document processing capabilities.
EDMS FileNet	Electronic Document Management System (EDMS) FileNet is PennDOT's enterprise standard solution for long-term electronic document and content management based on IBM FileNet (currently Panagon and soon to be available with P8).
EDMS Scan Application	EDMS provides a configurable scan solution based on ImageAccess technology that supports scanning and indexing of content and loading of content to the FileNet repository. In addition to the stand-alone EDMS Scan application, scanning functionality can be embedded in applications with ImageAccess and some custom programming.
EDMS Web Service	EDMS provides a SOAP web service that is a wrapper service around FileNet. The web serviced allows developers to embed document management functionality, including search, import, retrieval, etc.) directly in their line-of-business applications.
PDIF BI Portal	The PennDOT Data Integration Facility (PDIF) BI Portal is a web-based portal and a development platform for BI and end-user reporting solutions. It is a .NET application and integrates with reporting content (e.g. Crystal Reports, Excelcius and WEBI) published to Business Objects Business Intelligence (BOBI) server.
PDIF BOBI Gateway	PennDOT Data integration Facility (PDIF) BOBI Gateway is a REST web-service API that enables secure, tight integration of Crystal Reports content on the Business Objects Business Intelligence Enterprise server within business applications.

PDIF Enterprise Data Warehouse	The PennDOT Data Integration Facility (PDIF) Enterprise Data Warehouse is PennDOT's enterprise data warehouse in Oracle that integrates data from many disparate source systems for end-user reporting and analysis. The PDIF DW contains staging, ODS, OLAP and enterprise metadata stores.
PDJF Java Application Framework	PDJF is a custom application framework for rapid development and delivery of high-quality solutions in Java/J2EE.

7 STANDARD: Enterprise Infrastructure

7.1 Definition

Enterprise Infrastructure refers to all of the server hardware, systems software, networks, workstations and hosting facilities that support the organization. Server hardware is organized into managed pre-production and production environments and deployed as shared resources to be leveraged by many IT solutions. Defining standards for *Enterprise Infrastructure* is essential for promoting awareness so the organization can maximize rationalization and reuse.

The remainder of this section identifies PennDOT's standard *Enterprise Infrastructure*

7.2 Enterprise Servers

Server	Description
Business Objects	Business Objects v3.x hosted on Windows Server 2008 servers in the Enterprise Data Center in Harrisburg, PA. Includes multiple sets of Development, Test and Production environments.
Informatica PowerCenter	Informatica PowerCenter 9.x hosted on Windows Server 2008 in the Enterprise Data Center in Harrisburg, PA. Includes Development, Test and Precaution environments.
Microsoft Internet Information Services (IIS)	IIS 7.5 hosted on Windows Server 2008 in the Enterprise Data Center in Harrisburg, PA. Includes Sandbox, Development, System Test, UAT and Production environments.
Oracle Database	Oracle 11g hosted on zLinux on the IBM Mainframe in the PACS facility in Ashburn, Virginia. Includes Development, System Test, UAT and Production environments.
Microsoft SQL Server Database	SQL Server 2008 hosted on Windows Server 2008 in the Enterprise Data Center in Harrisburg, PA. Includes Development, System Test, UAT and Production environments.
IBM WebSphere Application Server	IBM WebSphere Application Server (WAS) 7.x and 8.x hosted on Windows Server 2008 in the Enterprise Data Center in Harrisburg, PA and on zLinux on the IBM Mainframe in the PACS facility in Ashburn, Virginia. Includes, at a minimum, Sandbox, Development, UAT and Production environments.
IBM Integration Bus (IIB)	IBM Integration Bus 10 hosted on zLinux on the IBM Mainframe in the PACS facility in Ashburn, Virginia. Includes Development, System Test, UAT and Production environments.
IBM Mainframe	IBM Mainframe hosted in the PACS facility in Ashburn, Virginia. Hosts zLinux guests that support Oracle database, IBM WebSphere Application Server (WAS) and IBM Integration Bus (IIB) as well as legacy IMS and DB/2 databases and COBOL applications. System Configuration is as follows: • zEC12 Enterprise server model 2827-504 • z/OS and z/VM Operating Systems • z/OS 3 Logical Partitions: Production Applications, Development & Test, Sandbox • z/VM 3 Logical Partitions: Production z/Linux guests, Pre-prod z/Linux guests, Tivoli Monitoring

7.3 Hosting Facilities

Facility	Description
PACS	Commonwealth's PA Compute Services (PACS) facility in Ashburn, Virginia
EDC	Commonwealth's Enterprise Data Center (EDC) facility in Harrisburg, PA

7.4 Network Components

PennDOT's network infrastructure connects thousands of client devices in hundreds of locations throughout the Commonwealth.

LAN

- Ethernet, TCP/IP, 100MB-1GB to desktop

WLAN

- PennDOT provides 802.11n connectivity for PennDOT issued wireless devices.

WAN

- Core MPLS and CopaNET
- Remote Sites MPLS ranging from 1.5Mbps to 1Gbps and site to site VPN connections.
- Business Partner Connections range from 1 Mbps to 1 Gbps and includes some site to site VPN connections.
- Cellular Private IP Network based on Verizon Wireless MPLS.

7.5 URL Branding – Application Web Site Naming Convention (DNS)

The DNS naming standard for websites is **PENNDOT.GOV** for both internal (only on the COPA network) and external (the world). The following naming conventions examples are provided to PennDOT teams for guidance when selecting a URL/website naming convention.

Sandbox Website: ECS**SBX**.PENNDOT.GOV
Development Website: ECS**DEV**.PENNDOT.GOV
System Test Website: ECS**SYST**.PENNDOT.GOV
User Acceptance Website: ECS**UAT**.PENNDOT.GOV
Production Website: ECS.PENNDOT.GOV

Note all sites will need to be name resolvable outside of the Commonwealth of PA network pending their intended use. For example, a proof of concept type website in the sandbox environment should not be resolvable to the entire internet.

Name Resolution for	PENNDOT.GOV zone (OA)	PENNDOT.GOV zone (PennDOT)
Anyone on the internet	x	
Anyone on COPA		x
Anyone anywhere	x	x

7.6 Standard Workstation

PennDOT provisions employees with Windows-based desktop PC's and/or laptops.

Hardware

- Desktop PC – Intel Core i7-3770 3.4GHz, 128 GB HDD, 8GB DDR3 RAM
- Laptops – Intel Core i7-3720QM 2.6GHz, 256GB HDD, 8GB DDR3 RAM

Software

- Operating System – Microsoft Windows
- Office Productivity – Microsoft Office
- Internet Browser - Microsoft Internet Explorer
- Microsoft .Net 4.0
- Java Runtime 1.6.0_35
- Panagon Viewer (IDM Viewer) 4.0.2 Hot Fix 8
- Corel GIS Active-X Viewer 7.1
- Adobe Acrobat Reader XI Patch 3
- McAfee VirusScan Enterprise 8.8 Patch 4
- WinZip 18.5 Licensed
- SAP GUI 7.30 Patch 9
- Adobe Flash Player 13
- Adobe SVG Viewer
- Cisco AnyConnect (Laptops only)

8 STANDARD: Enterprise Technologies

8.1 Definition

Enterprise Technologies are those generally available hardware and/or software products that are used as the most basic building blocks for IT solutions. Not all technologies used by PennDOT are standardized, as many of them are used in narrow ways and are not of critical importance. Only those most critical technologies that have a significant impact on the IT landscape of the organization are subject to standardization and are thus identified as *Enterprise Technologies.*

In a perfect world, the organization would choose a single *Enterprise Technology* for each solution need (e.g. SQL Server as the single *Enterprise Technology* for RDBMS). With large organizations where IT solutions are acquired and/or built from many different sources, this is not possible. The goal of technology standardization and rationalization is to limit the unchecked proliferation of different technologies for performing identical or similar functions as opposed to mandating that there be only one.

The remainder of this section identifies PennDOT's standard *Enterprise Technologies.*

8.2 List of Enterprise Technologies

PennDOT maintains a listing of our current standard *Enterprise Technologies* in the IT Asset Management (ITAM) Portal http://itam.pdot.state.pa.us/. From the ITAM Portal, PennDOT staff can generate the *PennDOT Enterprise Technology Standard (ITLM008)* report. This report is the list of PennDOT's standard *Enterprise Technologies* that includes: technology name, version, category, manufacturer, platform, description and lifecycle classification

PennDOT's standard *Enterprise Technologies* as of March 7, 2017 are listed in the report below:

PennDOT Enterprise Technology Standard

This report shows the active enterprise technologies that are identified as PennDOT Standard

Thursday, March 23, 2017

pennsylvania DEPARTMENT OF TRANSPORTATION

TECHNOLOGY	VERSION	OS PLATFORM	MFR NAME	CLASSIFICATION	LIFECYCLE
.NET Framework	4.5.1	Windows Server	Microsoft	App Dev Environment	Current
Access Gateway	12.5.2	Windows Server	CA	Identity and Access Mgmt	Current
Adobe Reader	11	Windows	Adobe	Office Productivity	Current
ArcGIS Server	10.2	Windows Server	ESRI	App Server	Current
AXIS Camera Management	2	Windows Server	AXIS Communications	Video Software	Current
Azure App Service	N/A	Cloud (PaaS)	Microsoft	App Server	Research/Emerging
Azure Blob Storage	N/A	Cloud (PaaS)	Microsoft	Other	Research/Emerging
Azure Data Factory	N/A	Cloud (PaaS)	Microsoft	ETL Tools	Research/Emerging
Azure HD Insights	N/A	Cloud (PaaS)	Microsoft	Reporting	Research/Emerging
Azure ML	N/A	Cloud (PaaS)	Microsoft	Reporting	Research/Emerging
Azure SQL	N/A	Cloud (PaaS)	Microsoft	DBMS	Research/Emerging
BusinessObjects Enterprise	4.2	Windows Server	SAP	Reporting	Current
Captiva InputAccel Server	7.5	Windows Server	EMC	Electronic Doc Mgmt System	Current
Crystal Reports	2008	Windows	SAP	Reporting	Current
Data Center Network Manager	5.2	Windows Server	Cisco	Infrastructure Monitoring	Current
DataPower	6.0.1.0	Windows Server	IBM	Other	Current
Domino Designer	8.5	Windows	IBM	App Dev Language	Current
FileNet Process Engine for Windows	5.2	Windows Server	IBM	Electronic Doc Mgmt System	Current
Finalist	9.1.0	z/OS	Group 1 Software	Application Interfaces	Current
GlobalScape EFT	7.3.4	Windows Server	GlobalScape, Inc.	Midware Technologies	Current

TECHNOLOGY	VERSION	OS PLATFORM	MFR NAME	CLASSIFICATION	LIFECYCLE
HTTP Server on Windows	8	Windows Server	IBM	Web Server	Current
IBM Integration Bus (IIB)	10	z/Linux	IBM	Midware Technologies	Current
IdentityMinder	R12	Windows Server	CA	Identity and Access Mgmt	Current
IIS	7.5	Windows Server	Microsoft	Web Server	Current
IMS Connect	13	z/OS	IBM	Midware Technologies	Current
Infoprint Server	2.1	z/OS	IBM	Application Interfaces	Current
Informatica PowerCenter	9.5.0	Windows Server	Informatica	ETL Tools	Current
Internet Explorer	11	Windows	Microsoft	Internet Browser	Current
Java Enterprise Edition (EE)	6	Multiple	Oracle	App Dev Language	Current
Java Enterprise Edition (EE)	7	Multiple	Oracle	App Dev Language	Research/Emerging
Linux (Red Hat)	7.1	Linux	Red Hat	Operating System	Current
Lotus Notes	8.5	Windows	IBM	Developer Tools	Current
Microsoft Office	Office 365	Windows	Microsoft	Office Productivity	Current
Oracle Windows	11g	Windows Server	Oracle	DBMS - Client	Current
Oracle z/Linux	11g	z/Linux	Oracle	DBMS	Current
Oracle z/Linux	12c	z/Linux	Oracle	DBMS	Research/Emerging
Power BI	N/A	Cloud (SaaS)	Microsoft	Reporting	Research/Emerging
Rational AppScan Source Edition for Security	8.5	Windows	IBM	Developer Tools	Current
Rational Functional Tester	8.5	Windows	IBM	App Testing Tool	Current
Rational Host on Demand	11	Windows Server	IBM	Emulator - 3270	Current
Rational Performance Tester	8.5	Windows	IBM	Developer Tools	Current
Rational Quality Manager	4.1	Windows	IBM	Developer Tools	Current
Rational Requirements Composer	4.1	Windows	IBM	Developer Tools	Current
Rational Software Architect	8.5	Windows	IBM	Developer Tools	Current

TECHNOLOGY	VERSION	OS PLATFORM	MFR NAME	CLASSIFICATION	LIFECYCLE
Rational Team Concert	5	Windows Server	IBM	Developer Tools	Current
RoboHelp	10	Windows Server	Adobe	Developer Tools	Current
SCCM	2012	Windows Server	Microsoft	Infrastructure Monitoring	Current
SCOM	2012	Windows Server	Microsoft	Infrastructure Monitoring	Current
SharePoint	2010 SP 1	Windows Server	Microsoft	Collaboration	Current
SharePoint	2016	Windows Server	Microsoft	Collaboration	Research/Emerging
SiteMinder	12.51	Windows Server	CA	Identity and Access Mgmt	Current
SQL Server	2014	Windows Server	Microsoft	DBMS	Current
Storage Foundation for Windows (Server Components)	6	Windows Server	Veritas	SAN Tools	Current
Team Foundation Server (TFS)	2015	Windows Server	Microsoft	App Dev Environment	Current
Tivoli Monitor	0	z/Linux	IBM	Infrastructure Monitoring	Current
Tivoli Monitoring Agents Omegamon zOS	5.3	z/OS	IBM	Infrastructure Monitoring	Current
Tivoli Monitoring Agents x86 for Linux Operating Systems	6.3	Linux	IBM	Infrastructure Monitoring	Current
Tivoli Storage Manager	7.1.0	Windows Server	IBM	Backup Tools - Server	Current
Tivoli Storage Manager Client	7.1.0	Windows	IBM	Backup Tools - Server	Current
Tivoli Storage Manager Extended Edition	6.3	Windows Server	IBM	Backup Tools - Server	Current
Tivoli Storage Manager for Databases	6.3	Windows Server	IBM	Backup Tools - Server	Current
Tivoli Storage Manager for Mail	6.3	Windows Server	IBM	Backup Tools - Server	Current
Tivoli Workload Scheduler for z/Linux	zcentric 8.5.1	z/Linux	IBM	Batch Job Scheduler	Current
Tivoli Workload Scheduler for z/OS	9.3.0	z/OS	IBM	Batch Job Scheduler	Current
Visual Studio Team Services	N/A	Cloud (SaaS)	Microsoft	App Dev Environment	Current
VMware vCenter Server	5	Windows Server	EMC	Virtualization Server	Current
VMware vSphere Client	5	Windows	EMC	Virtualization Server	Current

TECHNOLOGY	VERSION	OS PLATFORM	MFR NAME	CLASSIFICATION	LIFECYCLE
Web Sphere MQ Client .NET	7.0		IBM		Current
Websphere Application Server Linux RedHat	8.5	Linux	IBM	Web Server	Current
WebSphere Liberty Profile (x86 Linux)	16.0.0.3	Linux	IBM	Web Server	Current
WebSphere MQ for z/Linux	8.0.0.5	z/Linux	IBM	Midware Technologies	Current
Windows	7	Windows	Microsoft	Operating System	Current
Windows Server	2012 R2	Windows Server	Microsoft	Operating System	Current
zLinux/SLES	SLES 11	z/VM	IBM	Operating System	Current
zOS	2.1	z/OS	IBM	Operating System	Current

8.3 Technologies Expressly Not Supported

The following technologies are expressly not supported for use in new and/or significantly modified IT solutions, either because they present operational and support challenges or because they are prohibited by Commonwealth of Pennsylvania OA/OIT enterprise standards.

1. Any technologies that are not standards as identified by PennDOT or the Commonwealth of Pennsylvania OA/OIT,
2. Any technologies with an IT Lifecycle Classification of “Retire” or “Contain” by either PennDOT or the Commonwealth of Pennsylvania OA/OIT,
3. Any technologies with an IT Lifecycle Classification of “Emerging” by the Commonwealth of Pennsylvania OA/OIT,
4. Any open source, shareware, freeware, public domain or other non-commercial technologies (excluding application frameworks, such as Spring, Hibernate, etc.) unless they are identified as PennDOT or Commonwealth of Pennsylvania OA/OIT standard, and
5. Client-side Java SE unless it is packaged and deployed with an IT solution and isolated from any other Java SE clients.

9 STANDARD: Hosting Requirements

The following requirements ***must*** be met when Commonwealth of Pennsylvania data and/or IT services are implemented on hardware and/or software that is not owned and managed by Pennsylvania Department of Transportation staff. These requirements apply to any external hosting arrangements and Software as a Service (SaaS) Information technology solutions.

A. Hosting Requirements

1. The selected Offeror shall supply all hosting equipment (hardware and software) required for performance of the Contract.
2. The selected Offeror shall provide secure access to all levels of users via the internet.
3. The selected Offeror shall use commercially reasonable resources and efforts to maintain adequate internet connection bandwidth and server capacity.
4. The selected Offeror shall maintain all hosting equipment (hardware and software) and replace as necessary to maintain compliance with the Service Level Agreements as described in the service level agreement (SLA) appendix of the RFP\RFQ.
5. The selected Offeror shall monitor, prevent and deter unauthorized system access. Any and all known attempts must be reported to the Commonwealth within the timeframe set out by the RFP. In the event of any impermissible disclosure, loss or destruction of Confidential Information, the receiving Party must immediately notify the disclosing Party and take all reasonable steps to mitigate any potential harm or further disclosure, loss or destruction of such Confidential Information. In addition, pertaining to the unauthorized access, use, release, or disclosure of data, the selected Offeror shall comply with state and federal data breach notifications regulations and is to report security incidents to the Commonwealth within one (1) hour of when the selected Offeror knew of such unauthorized access, use, release, or disclosure of data.
6. The selected Offeror shall allow the Commonwealth or its delegate, at times chosen by the Commonwealth, to review the hosted system's location and security architecture.
7. The selected Offeror staff, directly responsible for day-to-day monitoring and maintenance, shall have industry standard certifications applicable to the environment and system architecture used.
8. The selected Offeror shall locate servers in a climate-controlled environment. Offeror shall house all servers and equipment in an operational environment that meets industry standards including climate control, fire and security hazard detection, electrical needs, and physical security.
9. The selected Offeror shall examine system and error logs daily to minimize and predict system problems and initiate appropriate action.
10. The selected Offeror shall completely test and apply patches for all third-party software products before release.
11. Offerors shall provide a successfully passed SSAE- 16 SOC2 audit report, conducted by an independent certified public accounting firm, subject to the approval of the Department, as part of its proposal, and the selected Offeror shall provide a SSAE-16 audit reports annually.

B. System Availability

1. The selected offeror shall make available the system and any custom software as established in the requirements section of the request for proposal\request for quotation.
2. The selected offeror shall perform routine maintenance during the planned weekly maintenance period as described in the requirements section of the RFP\RFQ. Routine maintenance shall include, but is not limited to, server upgrades/patching, software upgrades/patching and

hardware maintenance. If defined as a requirement in the RFP\RFQ, In order to maintain system availability, the Offeror is expected to rollover to a backup site during maintenance periods.

3. The selected Offeror shall perform non-routine maintenance at a mutually agreeable time as defined in the RFP\RFQ..
4. From time to time, emergency maintenance may be required to bring down the system. In such situations, if possible, the selected Offeror shall give advance notice, before the system goes down for maintenance, to the Commonwealth. The selected Offeror will limit the emergency maintenance to those situations which require immediate action of bringing down the system that cannot wait for the next scheduled maintenance period. If defined as a requirement in the RFP\RFQ, It is expected that the Offeror will rollover to a backup site during any such emergency maintenance.

C. Security Requirements

1. The selected Offeror shall conduct a third party independent security/vulnerability assessment at its own expense on an annual basis and submit the results of such assessment to the Commonwealth within three (3) business days.
2. The selected Offeror shall comply with Commonwealth directions/resolutions to remediate the results of the security/vulnerability assessment to align with the standards of the Commonwealth.
3. The selected Offeror shall use industry best practices to protect access to the system with a firewall and firewall rules to prevent access by non-authorized users and block all improper and unauthorized access attempts.
4. The selected Offeror shall use industry best practices to provide system intrusion detection and prevention in order to detect intrusions in a timely manner.
5. The selected Offeror shall use industry best practices to provide virus protection on all servers and network components.
6. The selected Offeror shall limit access to the system and servers and provide access only to those staff that must have access to provide services proposed.
7. The Selected Offeror will provide all Services, using security technologies and techniques in accordance with industry best practices and the Commonwealth's security policies, procedures, and requirements, including those relating to the prevention and detection of fraud and any other inappropriate use or access of systems and networks.

D. Data Storage

1. The selected Offeror shall use industry best practices to update all systems and third party software security patches to reduce security risk. The Selected Offeror shall protect their systems with anti-virus, host intrusion protection, incident response monitoring and reporting, network firewalls, application firewalls, and employ system and application patch management to protect its network and customer data from unauthorized disclosure.
2. The selected Offeror shall be solely responsible for all data storage required.
3. The selected Offeror shall take all necessary measures to protect the data including, but not limited to, the backup of the servers on a daily basis in accordance with industry best practices and encryption techniques.
4. The Selected Offeror agrees to have appropriate controls in place to protect critical or sensitive data and shall employ stringent policies, procedures, and best practices to protect that data particularly in instances where sensitive data may be stored on a Selected Offeror controlled or owned electronic device.

5. The selected Offeror shall utilize a secured backup solution to prevent loss of data, back up all data every day and store backup media. Storage of backup media offsite is required. Stored media must be kept in an all-hazards protective storage safe at the worksite and when taken offsite. All back up data and media shall be encrypted.

E. Disaster Recovery

1. The selected Offeror shall employ reasonable disaster recovery procedures to assist in preventing interruption in the use of the system.

F. Payment Card Industry (PCI) Compliance

Note: This section only applies if the RFP\RFQ applies to Payment Card Industry (PCI) data.

1. The Selected Offeror is obliged to adhere to the Payment Card Industry Data Security Standard (PCI DSS) if it processes payment card data. Moreover, The Selected Offeror certifies that their Information Technology practices conform to and meet current PCI DSS standards as defined by The PCI Security Standards Council at

   https://www.pcisecuritystandards.org/security_standards/index.php.

2. The Selected Offeror will monitor these PCI DSS standards and its Information Technology practices and the Selected Offeror will notify the Commonwealth within one (1) week, if its practices should not conform to such standards. The SELECTED OFFEROR will provide a letter of certification to attest to meeting this requirement and agrees to the Commonwealth's right-to-audit either by Commonwealth or external 3rd party auditors.
3. Selected Offeror agrees that it may (1) create, (2) receive from or on behalf of Commonwealth, or (3) have access to, payment card records or record systems containing cardholder data including credit card numbers (collectively, the "Cardholder Data"). Selected Offeror shall comply with the Payment Card Industry Data Security Standard ("PCI-DSS") requirements for Cardholder Data that are prescribed by the payment brands (as appropriate including Visa, MasterCard, American Express, Discover), as they may be amended from time to time (collectively, the "PCIDSS Requirements"). Selected Offeror acknowledges and agrees that Cardholder Data may only be used for assisting in completing a card transaction, for fraud control services, for loyalty programs, or as specifically agreed to by the payment brands, for purposes of this Agreement or as required by applicable law.

G. Adherence to Policy

1. The selected Offeror support and problem resolution solution shall provide a means to classify problems as to criticality and impact and with appropriate resolution procedures and escalation process for each classification of problem.
2. The selected Offeror shall abide by all of the Commonwealth’s policies (Information Technology Policies (ITPs)).
3. The Selected Offeror shall comply with all pertinent federal and state privacy regulations.

H. Closeout

1. When the contract term expires or terminates, and at any other time at the written request of the Commonwealth; the selected Offeror must promptly return to the Commonwealth all its data (and all copies of this information), in a format agreed to by the Commonwealth, that is in the selected Offeror's possession or control.