APPENDIX J

RFA 38-22 Addendum 1

pennsylvania
OFFICE OF ADMINISTRATION

Computing Services Requirements (CSR)

Service Organizations and/or Offerors that include Computing Services as described in ITP-SEC040 shall undergo a review as part of the Commonwealth's Computing Services Use Case (CUC) review process.

ITP-SEC040 establishes guidance on the management of Service Organizations and establishes requirements for the procurement and use of any non-Commonwealth Hosted Applications and/or Services (Computing Services). Solutions using traditional hosting methods and/or cloud computing are both applicable for completion of the Computing Services Requirements (CSR) document.

The purpose of this document is to gain the necessary information from the Service Organization or Offeror (if new solicitation) to fully understand and evaluate the Computing Services being proposed.

Guidelines for required documents and completing the CSR as follows:

1) Service Organizations and/or Offerors shall submit the following documents: 1. this CSR document; 2. relevant SOC reports; 3. Accessibility Conformance Reports (ACRs); 4. Vulnerability Assessment Executive Summary; 5. Business Continuity Plan (BCP); 6. Incident Response Plan (IRP); 7. Regulatory Compliance Certifications (e.g., HIPAA, etc.); 8. and other documents as applicable to the services being provided.
2) Service Organizations and/or Offerors shall provide complete and detailed responses to the questions included in this CSR document. **Please be sure to completely address each REQ# below including all subparts to the questions.**
3) Service Organizations and/or Offerors shall describe if any part of the computing service is provided by other third-parties or subcontractors (Subservice Organizations). Details of how each Subservice Organization meets these requirements shall be incorporated into this document. Each response shall clearly indicate the responsibility of the Service Organization or Subservice Organization, respectively.
4) If using links in Response column, only direct links to language that responds specifically and solely to the questions shall be leveraged.

Name of Service Organization	
Name(s) of person who completed this CSR	
Date of Submission	

REQ#	Category	Question	Response
1	**General**	1. Please provide an overview of the Computing Service. 2. Please list the solution components, hosting environments, as well as the service organization and subservice organizations operating all aspects that are a part of the overall Computing Service. a. **Solution Component(s)** – SKU/Product Titles and/or Resources utilized by solution provider b. **Solution Environment(s)** – Name the hosting provider(s) used for any self-hosted, cloud service, and/or traditional hosting, etc. components. c. **Solution Operator(s)** – Organizational name of the Service Organization and any Subservice Organizations actively supporting the Computing Service.	1.1. Overview 1.2a. Solution Components - 1.2b. Solution Environments - 1.2c. Solution Operators -
2	**General**	1. Please describe whether the Computing Service is a dedicated single tenant or shared (multi-tenant) solution.	2.1. 2.2.

		2. If multi-tenant, please describe the security controls to isolate / separate each customer.	
3	**General**	1. Please describe Service Level Agreements (SLAs) included with the service that identify both the services required and the expected level of service including, but not limited to, the following: a. Availability b. Performance c. Incident Response Times d. Recovery (RTO/RPO) 2. Please describe or provide representative example(s) of service availability and performance metrics to be provided.	3.1.a. Availability - 3.1.b. Performance - 3.1.c. Incident Response Times - 3.1.d. Recovery (RTO/RPO) - 3.2.
4	**General**	1. Describe your controls for records retention and data destruction of data past retention period in accordance with ITP-SEC019 Policy and Procedures for Protecting Commonwealth Data and ITP-SEC015 Data Cleansing Policy. 2. Describe how you will confirm that the data has been destroyed. Commonwealth preference is certified letter(s) of confirmation at end of contract and quarterly for aged data.	4.1. 4.2.
5	**General**	1. Upon contract expiration or at any other time at the written request of the Commonwealth, all Commonwealth data (and all copies of this information) shall be returned to the Commonwealth in a format agreed to by the Commonwealth. What method(s) of export are available to the Commonwealth?	5.1.

6	**General**	1. Please provide current FedRamp Status (ready, in process, authorized, not yet applied) and level (Low, Moderate, or High). 2. If FedRamp status is "authorized," please provide details for the following: a. Service Model b. Deployment Model c. Impact Level d. Independent Assessor e. Authorization Date f. Service Description g. Agencies using this service	6.1. 6.2.a. 6.2.b. 6.2.c. 6.2.d. 6.2.e. 6.2.f. 6.2.g.
7	**General**	1. Indicate which of the following NIST Special Publications (a-f) are adhered to: a. NIST SP 800-53 Assessing Security and Privacy Controls in FIS organizations b. NIST SP 800-63 Digital Identity Guidelines c. NIST SP 800-92 Guide to Computer Security Log Management d. NIST SP 800-144 Guideline on Security and Privacy in Public Cloud Computing e. NIST SP 800-145 NIST Definition of Cloud Computing and Deployment Models f. NIST SP 800-146 NIST Cloud Computing Synopsis and Recommendations 2. Please indicate any other NIST guidelines applicable to the Computing Service.	Indicate Yes or No (a-f). 7.1.a. NIST SP 800-53 – 7.1.b. NIST SP 800-63 – 7.1.c. NIST SP 800-92 – 7.1.d. NIST SP 800-144 – 7.1.e. NIST SP 800-145 – 7.1.f. NIST SP 800-146 - 7.2. Other NIST SPs (if any) -

8	**Compliance (ITP-SEC040 CSR-S8)**	1. Please indicate if the Computing Service is subject to any of the following laws, regulations, and/or industry standards: a. CJIS and CHRIA for criminal history data b. HIPAA for health-related data c. IRS Pub 1075 and SSA for federal protected data d. PCI-DSS for financial data e. Other 2. Applicable certifications required if computing service is subject to any of the above.	8.1.a. CJIS and CHRIA – yes/no 8.1.b. HIPAA – yes/no 8.1.c. IRS Pub 1075 – yes/no 8.1.d. PCI-DSS – yes/no 8.1.e. Other (please specify) - 8.2. If any of the above are yes, provide copies of (or links to) certifications.
9	**CONUS Access Control (ITP-SEC040 CSR-L3)**	Access to provided systems and services and/or Commonwealth data shall be limited only to those staff located within CONUS. 1. Please describe your support model including after-hours support. 2. Please indicate if any support mechanism or staff are located outside of CONUS and describe in detail the offshore access required to provide the services. a. Indicate which countries, if any, outside of CONUS have access. b. Indicate what role(s) (by country) and what access to Commonwealth data and systems those role(s) will have. c. Indicate if logging is enabled to capture the date, time, named user, and nature of the offshore access (i.e., read-only or modify) and whether such logs are maintained and preserved according to applicable data protection law(s) and industry best practice standards.	9.1. 9.2. 9.2.a. 9.2.b. 9.2.c. 9.2.d.

		d. Indicate whether offshore staff are direct employees or are subcontracted staff. e. Indicate whether offshore staff have direct access to Commonwealth data or if the Commonwealth must grant access? If the Commonwealth must grant access, please provide request and approval process flow. f. Describe any additional protections in place with respect to Commonwealth data that vendors employees and/or subcontractors would have access to while OCONUS.	9.2.e. 9.2.f.
10	**CONUS Hosting (ITP-SEC040 CSR-L4)**	Data shall only be hosted, handled, or processed in physical locations within CONUS. 1. Please describe which data centers, including hosting providers and locations, are utilized. 2. Please provide a description of the physical security controls in place.	10.1. 10.2.
11	**System and Organization Controls (SOC) Reporting (ITP-SEC040 CSR-L5)**	1. Please provide appropriate Systems and Organizations Controls (SOC) report(s) which have been performed by an independent CPA-certified auditor and any required attestation letter for Subservices Organizations. Refer to section 5.1 System and Organization Controls (SOC) Reporting Requirements of ITP-SEC040 and to OPD-SEC040B System and Organization Controls (SOC) Reporting Procedure. **SOC 2 TYPE 2 Report** is required under the following conditions:	11.1. Relevant SOC 2 Type 2 reports to be provided and any required attestation letter for Subservices Organizations. If SOC 2 Type 2 is not available, please provide acceptable alternative (SOC 2 Type 1, ISO 27001 certificate, or a FedRAMP ATO). 11.2. Relevant SOC 1 Type 2 report to be provided (if applicable)

		• The service organization is **hosting, handling, or processing Class "C" Classified Records or Closed Records** as defined in ITP-INF015. Compliance mandated with federal or state audit requirements and/or policy. **SOC 1 TYPE 2 Report** is required under the following conditions: • The service organization is **hosting financial information** that could affect or have a material impact on a Commonwealth agency's financial statements and/or reporting. • Compliance mandate for federal or state audit requirements and/or policy. • A third-party provides financial service(s) (such as, but not limited to, payroll processing, accounts receivable, payable, or collection service).	
12	**Accessibility Standards (ITP-SEC040 CSR-A1)**	1. Per ITP-ACC001, please submit Accessibility Conformance Reports (ACRs) using the most current version of the Voluntary Product Accessibility Template (VPAT) for the Computing Service(s). • The VPAT template should be filled out in its entirety and include testing methodology, conformance level, and remarks for any partially supported or non-supported level. • If ACR(s) are submitted, using an older version of the VPAT, Offeror/Contractor should provide an explanation as to why the most current version is not being used.	12.1. Applicable Accessibility Conformance Reports (ACRs) provided (yes/no) -

13	**System Monitoring Audit Logging (ITP-SEC040 CSR-S1)**	1. Please review and evaluate the system monitoring and audit logging requirements listed in ITP-SEC040 **Section 5.3** and describe which apply and how they are being addressed as part of the Computing Service. a. Indicate any additional monitoring and logging that is also included. 2. Please describe which system monitoring and audit logs are available to the customer and indicate how they are made available to the Commonwealth Information Security Officers (ISOs). 3. Please indicate if authorized direct access, available only upon request, or other. 4. Please describe if any dashboards and/or analytics are in place for Commonwealth ISO use. 5. Please describe continuous monitoring strategy, including Security Operation Center (SOC) processes and procedures.	13.1 13.1.a 13.2 13.3 13.4 13.5
14	**Boundary Protection / Network Protection (ITP-SEC040 CSR-S2)**	1. Please provide a high-level network / architecture diagram showing what security and technical controls are performing the network segmentation within the service. If information requested below is not included on the diagram provided, please include detailed responses. a. If solution spans more than one hosting environment (such as integration to Commonwealth managed environments	14.1. Diagram provided (yes/no) - 14.1.a.i. Included in diagram (yes/no) or details here -

		and/or across multiple hosting providers), please include the following: i. What solution components are deployed in each environment? ii. What data resides in each environment? b. Diagram shall include the following if included with the service: i. web application firewall ii. perimeter, border, and/or network firewall iii. VPN tunnel(s) iv. security zone boundary controls c. Diagram shall include the direction of connectivity (specify whether initiated inbound, outbound, or both) and specifications for API calls, protocols, ports, etc. 2. Please describe how data segregation (physically or logically) of Commonwealth data from non-Commonwealth data is guaranteed.	14.1.a.ii. Included in diagram (yes/no) or details here - 14.1.b.i. Included in diagram (yes/no) or details here - 14.1.b.ii. Included in diagram (yes/no) or details here - 14.1.b.iii. Included in diagram (yes/no) or details here - 14.1.b.iv. Included in diagram (yes/no) or details here - 14.1.c. Included in diagram (yes/no) or details here - 14.2.

15	**Exploit and Malware Protection (ITP-SEC040 CSR-S3)**	1. Please indicate which Exploit and Malware security controls are included in the Computing Service. a. File Monitoring controls b. Antivirus controls c. Cloud Aware IDS/IPS d. DLP controls e. Forensic controls f. Advanced Persistent Threat (APT) controls g. Other provided exploit and malware security controls	Please indicate yes or no if exploit and malware security controls listed are implemented as required (a-f). If control(s) not implemented, please indicate timeline for implementation and/or explain why not available. 15.1.a. File Monitoring controls – 15.1.b. Antivirus controls – 15.1.c. Cloud Aware IDS/IPS – 15.1.d. DLP controls – 15.1.e. Forensic controls – 15.1.f. Advanced Persistent Threat (APT) controls – 15.1.g. List any other exploit and malware security controls included with service.
16	**Encryption (ITP-SEC040 CSR-S4)**	Encryption technical controls are required to protect data in transit and data at rest. Commonwealth policy requires the vendor to comply with ITP-SEC031 and ITP-SEC019 encryption policies and minimum standards. 1. Please indicate which encryption (e.g., TLS 1.2+, key vaults, etc.) are used for data in transit? 2. Please indicate which encryption are used for data at rest (e.g., AES 256, column level, etc.)?	16.1. 16.2. 16.3.

		3. Please indicate if any portion of the computing service is not encrypted.	
17	**Identity and Access Management (ITP-SEC040 CSR-S5)**	Computing Services shall utilize Commonwealth Identity and Access Management (IAM) services, and where applicable Multi-Factor Authentication (MFA) to authenticate users that require access to the proposed service. 1. If cloud service is accessed by Commonwealth employees, please confirm Microsoft Azure Active Directory (AAD) will be utilized. 2. If cloud service is accessed by residents and/or business partners, please confirm Keystone Login will be utilized. 3. If Commonwealth authentication methods cannot be supported (for users identified in 1 and 2 above), please describe the technical controls used for authenticating users, multifactor services, provisioning and deprovisioning users, identity interaction and nonrepudiation needs for admins, internet user, internal users, etc. 4. For Service Organization staff, please describe authentication method, MFA use, internal reporting and audit mechanism for new staff, access changes, and deprovisioning.	17.1. Microsoft Azure Active Directory (AAD)(Commonwealth employees) – yes/no 17.2. Keystone Login (Residents) – yes/no Keystone Login (Business Partners) – yes/no 17.3. Response required if “no” response was provided for 17.1 and/or 17.2. 17.4.
18	**Vulnerability Assessment (ITP-SEC040 CSR-S6)**	Third-party independent security/vulnerability assessments shall be conducted on an annual basis. 1. Confirm third-party vulnerability assessments are conducted on an annual basis during the	18.1. yes/no; if no, also provide explanation 18.2. Executive Summary attached – yes/no or described here:

		term of the contract. (Refer to ITP-SEC023 for guidance) 2. Please provide an Executive Summary of your most recent third-party vulnerability assessment. Summary shall include, at minimum, scan date(s), identified vulnerabilities, severity classifications, and remediation statuses.	
19	**Service Availability / Recovery (ITP-SEC040 CSR-S7)**	1. Please provide a copy of your B**usiness Continuity Plan** (BCP) that addresses the following (indicate N/A if not applicable to the service and/or if customer responsibility): a. Data / Database Recovery b. Application Recovery c. Operating System Recovery d. Infrastructure Recovery 2. Please describe your capability to do a complete restoration in the event of a disaster. 3. Please describe what tests are performed as part of your disaster recovery plan. 4. Please describe your capability to provide services during a pandemic event.	19.1. BCP attached – yes/no or described here: 19.1.a. – 19.1.b. – 19.1.c. – 19.1.d. – 19.2 19.3 19.4
20	**Security Incident Handling (ITP-SEC040 CSR-S9)**	1. Please provide a copy of your customer facing Incident Response Plan (IRP). IRP should include incident handling practices, severity classification levels, customer notification and escalation processes, expected timeframes from time of impact to resolution, etc. • Informational: The Commonwealth will provide escalation contacts and resource	20.1. IRP attached – yes/no or described here:

		account to be used for notification purposes.	
21	**Asset Inventory Management and Maintenance (ITP-SEC040 CSR-S10)**	1. Please confirm a complete, accurate, and update inventory is maintained and available to the Commonwealth upon request. 2. Please confirm no resources are used that are prohibited pursuant to federal laws and regulations or state laws, regulations, and procurement policy. 3. Describe how supply chain risks are appropriately managed for services being provided to the Commonwealth. 4. Please confirm notice will be provided to the Commonwealth for any changes to the inventory of resources used in the delivery of services being provided to the Commonwealth that would negatively impact regulatory compliance.	21.1. Detailed list can be in the form of a bullet list, a separate spreadsheet, or screenshot attachment or described here. 21.2. 21.3. 21.4.
22	**Patching (ITP-SEC040 CSR-S11)**	Service Organizations shall comply with requirements as outlined in ITP-SEC041 Section 5. 1. Please describe your patching policy and confirm whether all products are completely tested, and patches applied prior to service release. 2. Please confirm patching processes are in alignment with industry best practices for the update and patching of all applicable services being delivered to the Commonwealth.	22.1. 22.2.

23	**Capacity (ITP-SEC040 CSR-I4)**	1. Please provide capacity data associated with the computing service. If metrics were provided by the agency, values should be based on those metrics. If exact numbers are not available, please provide the following details: a. Typical values for organizations of similar size and type (note any known deviations in the expected PA implementation). b. Values for individual transactions and connections (ex: Each connection of type X consumes approximately 200 Kbps, or each transaction is approximately 5KB). c. For each of the above, provide details indicating whether such connections/transactions are batch processes (and expected/recommended intervals and run times) or not.	23.1. 23.1.a. 23.1.b. 23.1.c.
24	**Data Backup and Recovery (Hosting Terms)**	1. Please describe your backup and archival processes. 2. Please respond to the following: a. What is the length of time backups are available? b. Do you perform test restores and how frequently? c. What archival backup/restore capabilities are included in the services provided? d. Explain any shadowing or redundancy you have across multiple datacenters or repositories. e. Are copies of backups maintained at a separate location? If yes, for how long? f. List the different locations of backups or copies of backups including key	24.1 24.2.a. 24.2.b. 24.2.c. 24.2.d. 24.2.e. 24.2.f.

		management and storage for any backup encryption keys.	