APPENDIX U

Cloud Services Requirements

Offeror/Contractors proposing solutions that include cloud services must respond to the questions included in this document. The purpose of this document is to gain the necessary information from the Offeror/Contractor to fully understand and evaluate the cloud service being proposed.

Offeror/Contractor shall describe if any part of the proposed cloud service is provided by another third party or subcontractor. The ability of each subcontractor to meet these Cloud Services Requirements must be incorporated into this document.
Offeror/Contractor may add a separate attachment or denote responses as "Offeror/Contractor" or "Name of Subcontractor".

If using links in Offeror/Contractor Response column, please provide specific reference point that addresses the question.

REQ #	Category	Question	Offeror/Contractor Response
1	**General**	Offeror/Contractor shall provide an overview of the proposed cloud service. 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 proposed solution. · **Solution Component(s)** – SKU/Product Titles and/or Resources utilized by solution provider · **Solution Environment(s)** – Which public cloud provider, which private cloud stack, and/or who's datacenter for traditional hosting of components. · **Solution Operator(s)** – Organizational name of the Service Organization and any Subservice Organizations actively supporting the proposed solution.	

2	**General**	Offeror/Contractor shall describe if the proposed cloud service is a dedicated single tenant or shared (multi-tenant) cloud solution. If multi-tenant, Offeror/Contractor shall describe the security controls to isolate the tenants.	
3	**General**	Offeror/Contractor shall describe Service Level Agreements (SLAs) included with the proposed Cloud Service that identify both the services required and the expected level of service including, but not limited to, the following: · Availability · Performance · Disaster Recovery expectations (RTO/RPO) · Pandemic Recovery expectations · Location of the data Primary/Secondary (if applicable?) · Access to the data · Portability of the data (ability to move data to a different hosting provider) · Metrics used to measure the service, e.g. service level objectives	
4	**General**	Offeror/Contractor shall describe controls for record 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. Offeror/Contractor shall describe how they 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.	

5	**General**	Offeror/Contractor shall, upon contract expiration or at any other time at the written request of the Commonwealth, return to the Commonwealth all of its data (and all copies of this information) in a format agreed to by the Commonwealth. Offeror/Contractor shall provide method of export of Commonwealth data during the contract term.	
6	**General**	Offeror/Contractor shall provide current FedRamp Status (ready, in process, authorized, not yet applied) and level (Low, Moderate, or High). If FedRamp status is "authorized," Offeror/Contractor shall provide details for the following: · Service Model · Deployment Model · Impact Level · Independent Assessor · Authorization Date · Service Description · Agencies using this service	
7	**General**	Offeror/Contractor shall indicate if the following NIST guidelines are adhered to: · NIST SP 800-53 Assessing Security and Privacy Controls in FIS organizations · NIST SP 800-63 Digital Identity Guidelines · NIST SP 800-92 Guide to Computer Security Log Management · NIST SP 800-144 Guideline on Security and Privacy in Public Cloud Computing	

		· NIST SP 800-145 NIST Definition of Cloud Computing and Deployment Models · NIST SP 800-146 NIST Cloud Computing Synopsis and Recommendations Please also indicate if other NIST guidelines apply to the proposed cloud service.	
8	**Regulatory Compliance Verification**	Offeror/Contractor shall indicate if the proposed cloud service is subject to any of the following laws: · CJIS and CHRIA for criminal history data · HIPAA for health-related data · IRS Pub 1075 and SSA for federal protected data · PCI-DSS for financial data Offeror/Contractor shall provide certifications or letters of attestation for any deemed applicable to the proposed cloud service.	
9	**Access to Commonwealth specific systems, data, and services (ITP-SEC040 CSR-L3)**	Offeror/Contractor shall limit access to Commonwealth-specific systems, data and services and provide access only to those staff, located within CONUS, that must have access to provide services proposed. Offeror/Contractor shall describe their support model including after-hours support. Offeror/Contractor shall indicate if any support mechanism or staff are located outside of CONUS and describe in detail the offshore access required to provide services proposed. a) If OCONUS, Offeror/Contractor shall 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. b) If OCONUS support is required, Offeror/Contractor shall indicate whether offshore staff are direct employees or are subcontracted staff. c) If OCONUS, Offeror/Contractor shall indicate whether offshore staff have direct access to Commonwealth data or if the Commonwealth must grant access? If Commonwealth must grant access, please provide request and approval process flow. d) Please describe any additional protections in place with respect to Commonwealth data that vendors employees and/or subcontractors would have access to while OCONUS.	
10	**Data Hosting (ITP-SEC040 CSR-L4)**	Offeror/Contractor shall only host, store, or backup Commonwealth Data in physical locations within CONUS. · Offeror/Contractor shall describe which data centers are intended for use with the proposed cloud service. · Offeror/Contractor shall provide a description of the physical security measures in place within the proposed data centers. Describe both the physical data center access as well as server room and physical host access. Offeror/Contractor shall completely test and apply patches for all third-party software products before release.	

		· Offeror/Contractor shall describe how often the infrastructure, hardware, and software are upgraded, hardened, and patched and what notifications are provided to the customer.	
11	**System and Organization Controls (SOC) Reporting (ITP-SEC040 CSR-L5)**	Offeror/Contractor shall provide relevant SOC reports, which have been performed by an independent CPA-certified auditor, for the proposed cloud service. Reports should be submitted to the Contract Manager. Link to OPD_SEC040B SOC Reporting Procedures **SOC 1 TYPE II 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). **SOC 2 TYPE II Report** is required under the following conditions: · The service organization is **hosting, handling, or processing Class "C" Classified Records or Closed Records** as defined in ITP-SEC019 · Compliance mandated with federal or state audit requirements and/or policy.	

12	**Accessibility Standards (ITP-SEC040 CSR-A1)**	Offeror/Contractor shall comply with the Accessibility Standards in Section 6 of ITP-ACC001 for all provided products and services. · Offeror/Contractor shall submit a completed VPAT using the most current version of the VPAT template for the proposed cloud service(s). o 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. o If VPAT(s) are submitted, using an older version of the template, Offeror/Contractor should provide an explanation, as to why the most current version is not being used.	
13	**System Monitoring Audit Logging (ITP-SEC040 CSR-S1)**	Commonwealth policy requirements: · Audit logging must be enabled and accessible to the Commonwealth (Information Security Office or designee) · Verbose logging is required · Vendor must have ability to correlate events, create security alerts, and based on severity of event (critical, severe, high-level) send incident notifications to Commonwealth Information Security Officers (ISOs). · Maintain reports online for a minimum of 90 days and archive for a minimum of 1 year. If the Commonwealth requires longer retention periods, the longer retention requirement takes precedence and should be documented in the SOW. a) Offeror/Contractor shall review and evaluate the system monitoring and audit logging requirements listed in ITP-SEC040 **Section 4.2** and describe which apply and how they are being addressed as part of the proposed cloud	

		service. Offeror/Contractor shall also indicate if any additional monitoring and logging is included. b) Offeror/Contractor shall 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). Please indicate if authorized direct access, available only upon request, or other. c) Offeror/Contractor shall provide an example of the logs to show what level of detail is available. d) Offeror/Contractor shall describe if any dashboards and/or analytics are in place for Commonwealth ISO use. e) Offeror/Contractor shall provide examples of monthly reporting. f) Offeror/Contractor shall provide examples of annual reporting. g) Offeror/Contractor shall define their continuous monitoring strategy, including measures, metrics and control assessments including frequencies. h) Offeror/Contractor shall provide examples of log review, contingency plan testing, incident response plan testing and vulnerability scans i) Offeror/Contractor shall describe responses to assessment findings, threshold alerts, decisions to either mitigate, transfer, or accept risks related to identified vulnerabilities	

		j) Offeror/Contractor shall describe method of access for all of the above.	
14	**Data Segmentation Boundary Protection (ITP-SEC040 CSR-S2)**	Offeror/Contractor shall provide a network/architecture diagram showing what security and technical controls are performing the network segmentation within the cloud service offering. · If solution spans more than one hosting environment (such as integration to Commonwealth managed environments, or across multiple hosting providers), provide details on what solution components and data are deployed in which environment. · Include border gateway, perimeter and/or network firewall, web application firewall, VPN tunnels, security zone access as applicable to the solution. · Describe data encryption methods at rest and in transit across environments. · Include the direction of connectivity (specify whether initiated inbound, outbound, or both) and specifications for API calls, protocols, etc. · Estimated Transaction size, and frequency to be identified for each connection. Offeror/Contractor shall describe how data segregation (physically or logically) of Commonwealth data from non-Commonwealth data is guaranteed. Offeror/Contractor shall maintain the diagram throughout the contract term and provide updates if changes occur.	
15	**Exploit and Malware**	Offeror/Contractor shall provide and manage security controls. These are required to identify attacks, identify	

	Protection (ITP-SEC040 CSR-S3)	changes to files, protect against malware, protect user web services, Data Loss Prevention (DLP) and provide for forensic analysis. Offeror/Contractor shall describe which of these security controls are included in the proposed cloud service and how these additional controls would generate a notification to the Commonwealth. Please indicate if any are not used and also if any are used that are not listed below. o File Monitoring controls o Antivirus controls o Cloud Aware IDS/IPS o DLP controls o Forensic controls o Advanced Persistent Threat (APT) controls	
16	**Encryption (ITP-SEC040 CSR-S4)**	Commonwealth policy requires the vendor to comply with SEC031, and SEC019 encryption policies and minimum standards with the proposed cloud service. Encryption technical controls are required to protect data in transit and data at rest. Link to SEC031 Encryption Standards Data in Transit Link to SEC019 Protection of Commonwealth Data Offeror/Contractor shall describe what encryption protocols are used to secure data in transit, file uploads or transfers. Offeror/Contractor shall describe what encryption technology is used for data at rest. Describe how those encryption keys are managed.	

		Offeror/Contractor shall describe what encryption technology is used for data backup and recovery. Describe how those encryption keys are managed. If databases are used, describe what level of encryption is applied.	
17	**Identity and Access Management (ITP-SEC040 CSR-S5)**	Offeror/Contractor must provide technical controls for authenticating users, provisioning and deprovisioning users, identity interaction and nonrepudiation needs for admins, internet users, and internal users. Offeror/Contractor must describe reporting and audit mechanism for new staff, access changes, and deprovisioning of Offeror/Contractor staff. Offeror/Contractor must support use of Commonwealth Authentication services and Commonwealth Multi-Factor Authentication services. If cloud service is accessed by Commonwealth employees, Offeror/Contractor shall indicate if they can support Microsoft Azure Active Directory (AAD) or integration with ADFS. If cloud service is accessed by citizens or business partners, Offeror/Contractor shall indicate if they can support use of Keystone Login. If Offeror/Contractor cannot support use of Commonwealth authentication methods, Offeror/Contractor shall 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.	

18	**Vulnerability Assessment (ITP-SEC040 CSR-S6)**	Offeror/Contractor shall conduct third-party independent security/vulnerability assessments on an annual basis. Offeror/Contractor shall describe its vulnerability assessment practices for the proposed cloud service and indicate how the following requirements will be addressed: a) Offeror/Contractor shall ensure cloud hosted application(s) are securely coded, vetted, and scanned. b) Offeror/Contractor shall conduct quarterly vulnerability assessments, or sooner if due to compliance regulations or other requirements, or upon a major change to the solution. *c)* Offeror/Contractor shall conduct a vulnerability assessment on an annual basis during the term of the contract and shall provide a copy of the results to the Commonwealth. *(Refer to ITP-SEC021 and ITP-SEC023 for guidance)* d) Offeror/Contractor shall be able to identify and validate vulnerabilities required for remediation and provide a mitigation plan and timeline to the Commonwealth. e) Offeror/Contractor shall ensure patching is up to date.	
19	**Data Protection Recovery (ITP-SEC040 CSR-S7)**	Offeror/Contractor shall provide a **business continuity plan** that addresses the following (indicate N/A if not applicable to the proposed cloud service and/or if customer responsibility): o Data / Database Recovery o Application Recovery o Operating System Recovery o Infrastructure Recovery Offeror/Contractor shall describe its capability to do a complete restoration in the event of a disaster.	

		Offeror/Contractor shall describe what tests are performed as part of its disaster recovery plan. Offeror/Contractor shall describe its capability to provide services during a pandemic event.	
20	**Compliance (ITP-SEC040 CSR-S8)**	Offeror/Contractor shall describe its capability to meet compliance requirements if the proposed cloud service is subject to any regulations. At minimum, all offerings shall meet Commonwealth ITP requirements and NIST Moderate Level security controls specified in the Federal Information Processing Standards (FIPS) and Special Publications (SPs). NIST control enhancements shall also apply unless specified otherwise. The agency reserves the right to upgrade the NIST control level. The agency also reserves the right to mandate additional regulations or standards such as HIPAA, PCI, IRS, CMs/ARS, etc.	
21	**Security Incident Handling (ITP-SEC040 CSR-S9)**	Offeror/Contractor shall agree to monitor, prevent, and deter unauthorized system access as per the requirements outlined below and per the Requirement for Non-Commonwealth Hosted Applications/Services. Offeror/Contractor shall provide a copy of its 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.	

		· The Commonwealth will provide escalation contacts and resource account to be used for notification purposes.	
22	**Inventory (ITP-SEC040 CSR-S10)**	Offeror/Contractor shall describe how it maintains a complete, accurate, and up-to-date asset inventory of all resources involved in the proposed cloud service. Offeror/Contractor shall provide a detailed asset inventory list, including country of origin, that will be used for the proposed cloud service offering. The Commonwealth reserves the right to prohibit use of certain hardware based on risk. Include manufacturer, model numbers, processors, disk drives, database hardware, data center networking components (routers, switches, etc.), security devices (firewalls, etc.), load balancers, and any other hardware relevant to the delivery of the service. Offeror/Contractor shall provide notice to the Commonwealth for any changes to the asset inventory used to support the cloud service being provided to the Commonwealth that would impact regulatory compliance (refer to REQ#5 Regulatory Compliance Verification)	
23	**Capacity (ITP-SEC040 CSR-I4)**	Offeror or contractor shall provide capacity data associated with their offering. If metrics were provided by the agency, values should be based on those metrics. If exact numbers are not available, Offeror shall provide the following details: · Typical values for organizations of similar size and type (note any known deviations in the expected PA implementation).	

		· Values for individual transactions and connections (ex: Each connection of type X consumes approximately 200 Kbps, or each transaction is approximately 5KB). · For each of the above, provide details indicating whether such connections/transactions are batch processes (and expected/recommended intervals and run times) or not.	
24	**Data Backup and Recovery (Hosting Terms)**	Offeror/Contractor shall take all necessary measures to protect the data including, but not limited to, the backup of the servers on a daily and weekly basis in accordance with industry best practices and encryption techniques in accordance with Commonwealth retention requirements. Offeror/Contractor shall describe its backup and archival process including but not limited to the following: · What is the length of time backups are available? · Do you perform test restores? · What archival backup/restore/versioning is part of the agreement and what actions require any additional service fees? · Explain any shadowing or redundancy you have across multiple datacenters or repositories and if those data repositories are within the US and controlled by the vendor. · Is storage of backup media offsite provided? If so, for how long? · Location of backups and key management and storage for any backup encryption keys.	