



**Exhibit 2.1  
Description of Services**

**VA-240920-NTT: Managed Public Cloud Services**

**COMMONWEALTH OF VIRGINIA  
VIRGINIA IT AGENCY  
SUPPLY CHAIN MANAGEMENT**

7325 BEAUFONT SPRINGS DR.  
RICHMOND, VA, 23225

## Table of Contents

1.0	<a href="#">Introduction</a>
2.0	<a href="#">Cross-Functional Services</a>
2.1	<a href="#">General</a>
2.2	<a href="#">Engineering and Architecture</a>
2.3	<a href="#">Service Management Systems</a>
2.4	<a href="#">Cloud Broker Technology Integrator</a>
3.0	<a href="#">General Architecture</a>
3.1	<a href="#">General Architecture Requirements</a>
3.1.1	<a href="#">Design/Architecture Requirements</a>
3.1.2	<a href="#">Availability/Performance Requirements</a>
3.1.3	<a href="#">Capacity Requirements</a>
3.1.4	<a href="#">Continuity Requirements</a>
3.1.5	<a href="#">Technology Requirements</a>
3.1.6	<a href="#">Integration/Interoperability Requirements</a>
4.0	<a href="#">Security Requirements</a>
4.1	<a href="#">General Security Requirements</a>
4.1.1	<a href="#">Incident Response Security Requirements</a>
4.1.2	<a href="#">Security Integration</a>
4.1.3	<a href="#">Audit and Compliance</a>
4.1.4	<a href="#">User Authentication</a>
4.1.5	<a href="#">User Authorization</a>
4.1.6	<a href="#">Encryption at Rest</a>
4.2	<a href="#">List of Tools</a>
4.3	<a href="#">Security Approach</a>
4.4	<a href="#">Security Management</a>
4.5	<a href="#">Security Program</a>
4.6	<a href="#">Security Assessments</a>
4.7	<a href="#">Security Assessment by Third Parties</a>
4.8	<a href="#">Security Incident Management</a>
4.9	<a href="#">Security Clearance Management</a>
4.10	<a href="#">Security Clearance System</a>
4.11	<a href="#">Risk Management</a>
4.12	<a href="#">Risk Monitoring, Identification, and Reporting</a>
4.13	<a href="#">Risk Prevention and Mitigation</a>
5.0	<a href="#">MCS Program Management</a>
5.1	<a href="#">General MCS Program Management Requirements</a>
6.0	<a href="#">MCS Delivery Operations</a>
6.1	<a href="#">MCS Delivery Operations Requirements</a>
6.2	<a href="#">Operations, Maintenance, and Monitoring</a>
6.3	<a href="#">Patch Management</a>
6.4	<a href="#">Technical Support</a>
6.5	<a href="#">Capacity Management</a>
6.6	<a href="#">User Support</a>
6.7	<a href="#">Personnel/Clearance Management</a>
7.0	<a href="#">MCS Solution Management</a>
7.1	<a href="#">MCS Business Solution Management General Requirements</a>

7.2	<a href="#">Enhanced (Optional) Services</a>
8.0	<a href="#">Cloud Service Provider Specific Requirements</a>
8.1	<a href="#">Microsoft Azure</a>
8.2	<a href="#">Google Cloud Platform (GCP)</a>
8.3	<a href="#">Oracle Cloud Infrastructure (OCI)</a>
9.0	<a href="#">Assume Current Services</a>
9.1	<a href="#">Common Platform Services</a>
9.2	<a href="#">Server Services</a>
9.2.1	<a href="#">General Services</a>
9.3	<a href="#">Database Services</a>
9.4	<a href="#">Storage Services</a>
9.4.1	<a href="#">Storage Management</a>
9.4.2	<a href="#">Backup and Recovery Services</a>
9.4.3	<a href="#">Provisioning and De-Provisioning of Storage</a>
9.4.4	<a href="#">Security and Data Management</a>
9.5	<a href="#">Network Services Associated with Server/Platform/Storage Services</a>
9.5.1	<a href="#">General Requirements</a>
9.5.2	<a href="#">Planning and Design Services</a>
9.5.3	<a href="#">Operations and Maintenance</a>
9.5.4	<a href="#">Monitoring</a>
9.5.5	<a href="#">Network-based Appliance Services</a>
9.6	<a href="#">Security Functions</a>
9.6.1	<a href="#">General Integration</a>
9.6.2	<a href="#">Data Security</a>
9.7	<a href="#">OCI Specific Assumed Services</a>
9.8	<a href="#">Azure Specific Assumed Services</a>
9.9	<a href="#">GCP Specific Assumed Services</a>
10.0	<a href="#">Additional (Optional) Services</a>
11.0	<a href="#">SMM Responsibilities</a>
12.0	<a href="#">SMM Responses</a>

## VA-240920-NTT: Managed Public Cloud Services

### 1.0 Introduction:

This **Description of Services** sets forth the Services that Supplier will provide, as of the Commencement Date unless otherwise specified. Further, this Description of Services sets forth the processes and systems that Supplier will provide and describes Supplier's obligations to work with the other Suppliers to deliver integrated end-to-end Services to Customers.

Supplier confirms that unless otherwise specifically stated, it will provide a solution that supports all of the business processes described in this Description of Services and its Exhibits, and that all Services, unless otherwise specifically stated, are included within the Base Charges described in **Exhibit 4.0 (Pricing and Financial Provisions)**. Accordingly, Supplier also confirms that Customers will not incur any other Charges in relation to the Services described in this Description of Services.

#### **Scope: Managed Cloud Services Provider**

The purpose of this Request for Proposal ("RFP") is to solicit proposals for the provision of Managed Public Cloud Services for Commonwealth executive branch agencies declared by the legislature to be "in-scope" to VITA.

VITA is seeking three distinct Managed Public Cloud Services Providers (MCS) to join its multi supplier integrated platform to provide managed public cloud services for the following Cloud Service Providers (CSPs):

- Microsoft Azure
- Google GCP
- Oracle OCI

To ensure that VITA has adequate safeguards and redundancy within the managed cloud services environment and to reduce the risk of a single point of failure, it is the intention of VITA to make three (3) separate awards resulting in a one-to-one relationship between a single MCS awardee and a single CSP. One award for each of the three separate and distinct suppliers. For example, Supplier A would have a one-to-one relationship with MS Azure and Supplier B would have a one-to-one relationship with Google GCP. **Therefore, Offerors shall submit one (1) proposal for one (1) CSP in response to this RFP. Multiple submissions from a single offeror will remove the offeror from further consideration.**

VITA will be the owner of all CSP environments and tenants, in a VITA owned, contractor managed model. The MCS provider shall be an authorized partner of the CSP for which they submit a proposal, among other requirements.

The MCS provider will perform the following initial onboarding scope:

1. Assume current services as described in **Exhibit 2.1 (Description of Services – Managed Public Cloud Services), Tab 9.0 (Assume Current Services)** from the incumbent supplier for the CSP scope which the MCS is awarded a contract;
2. Successfully deliver a Remediation plan within 30 days of access to the Commonwealth’s environment;
3. Successfully deliver a Modernization plan within 90 days of access to the Commonwealth’s environment;
4. Process any Request For Solution (RFS) that the incumbent supplier has not fulfilled. A current list of planned projects is listed in **Exhibit 2.6 (Current-Planned Projects)**.

The MCS provider shall integrate into VITA's multi-supplier Service Management Platform as a Tier 1 Supplier. Detailed information regarding cross-functional responsibilities supporting the Service Management main processes are listed in **Exhibit 2.1 (Description of Services – Managed Public Cloud Services), Tab 2.0 (Cross-Functional Services), Tab 3.0 (Enterprise Architecture), Tab 4.0 (Security Requirements), and Tab 11.0 (SMM Responsibilities)** of this Exhibit are reflective of standards all Service Tower Suppliers shall support in VITA's MSI Platform. A detailed description of the Integrated Services Platform is available in the **Exhibit 1.0 (Integrated Services Platform)** in the RFP package.

VITA's Multi-Sourcing Service Integrator (“MSI”), Science Applications International Corporation (“SAIC”) will provide Cloud Broker Technology Integration (“CBTI”) services into which the MCS supplier shall integrate. The MCS Supplier(s) may bring a suite of tools to manage the cloud platform, but all MCS provided tools shall integrate into the MSI CBTI platform. MCS Supplier(s) may be asked to operate independent of the MSI's CBTI in some situations such as those found in **Tab 10.0 (Additional Services)**.

This MCS supplier will design, architect, develop, integrate, deploy, support, and optimize solutions based on RFS received.

The MCS Supplier will be required to provide end-to-end consulting services as part of its base offering. Agencies may request enhanced consulting services beyond the base offering for the development of comprehensive solutions that leverage applicable service components from the awarded CSP and their portfolio of services. The MCS supplier shall communicate the various ways the components of the cloud offerings can be assembled to solve business/Agency problems.

Offerors shall propose a cloud service management framework along with a staffed organization that oversees the fully managed use of the CSP's services. Suppliers shall have experience in providing solutions for varying lines of Business (Agencies), with differing needs, budgets, staff skills, and timeframes.

#### **Tab 5.0 (MCS Program Management)**

- Provide the strategic management skills, processes and tools necessary for the MCS provider's team to promote rapid delivery of compliant solutions with frictionless service integration among the incumbent suppliers.
- Provide capability to rapidly assess requirements based on customer needs, determine the implementation path, and articulate how the

CSP-sourced services are to be delivered and operated, with preference given to self-service delivery mechanisms.

**Tab 6.0 (MCS Delivery Operations)**

- The Operations Group will also provide implementation support, maintenance, and disaster recovery services. This team must meet all service level agreements on a monthly basis to achieve VITA's acceptance on all periodic critical deliverables.
- Refer to section 9 of this document for requirements for assuming current services from the incumbent supplier.

**Tab 7.0 (MCS Solution Management)**

- Engage with agency partners to determine business challenges facing application management teams, then provide solutions in support of those teams. This MCS architecture and engineering skills maps cloud services into the agency business solutions, while focusing on the most efficient, predictable, and cost-effective means to meet the business need.

Furthermore:

- Provide Services that are flexible, rapidly provisioned, cost effective, transparent, and elastic to meet VITA and Customer needs while preserving enterprise requirements such as Security and Compliance management.
- VITA is also open to any value-added services.

**Additionally, due to VITA's long-term strategic goals, Suppliers currently managing a CSP in VITA's MSI environment are not permitted to submit responses to this RFP.**

VA-240920-NTT: Managed Public Cloud Services

Ref #	Requirement	Comply (Y/N)	Supplier Response
	<p><b>2.0 CROSS-FUNCTIONAL SERVICES</b></p> <p><i>The Multisourcing Service Integrator (MSI) is the single organization in the Information Technology Infrastructure Services Program (ITISP) that is responsible for administration and coordination across all Service Tower Suppliers. The Supplier will work in integration with the MSI and other Suppliers and adhere to ITISP Governance to support the seamless delivery of Services to VITA and Customers.</i></p> <p><i>This Tab sets forth the cross-functional Services that the Supplier will provide, as of the Commencement Date unless otherwise specified. Further, this Description of Services sets forth the Supplier's obligations to work with the MSI to deliver integrated end-to-end Services to VITA and Customers.</i></p> <p><i>The Supplier's responsibilities common to all platforms are described in this Exhibit, which include:</i></p>		
1	Supplier will follow the processes and procedures covering the coordination, management, and reporting of the Integrated Suppliers across the Managed Environment as set forth in the Service Management Manual (SMM). See <b>Exhibit 1.0 (Integrated Services Platform)</b> and <b>Tab 11.0 (SMM Responsibilities)</b> for additional information regarding the Managed Environment and SMMs.	Y	
2	Establish Operating Level Agreements, and other supporting measures and controls with the MSI, as approved by VITA. In cooperation with the MSI, the Supplier is required to provide a set of actions in the Continual Service Improvements Register on a quarterly basis to establish and improve Operating Level Agreements (OLAs) and other supporting measures and controls with the MSI and other Service Tower Suppliers, as approved by VITA.	Y	
3	Deploy and integrate any tools and systems necessary to enable such processes, procedures and controls. Refer to section <b>2.3 (Service Management Systems)</b> , below.	Y	
4	Actively participate in information exchange between and among the Supplier, the MSI, other Service Tower Suppliers, VITA, Customers, and Third-Party Vendors to improve execution of the Service Management Manual processes.	Y	
5	Participate in the development and Documentation of processes, sub-processes and procedures for the Service Management Manual Processes with the MSI and other Service Tower Supplier(s), as approved by VITA.	Y	
6	Participate in in the Documentation of sub-processes, procedures and desk-level procedures for the Service Management Manual Processes that supports the individual environments within Customers' environments with the MSI and other Service Tower Suppliers.	Y	
7	Routinely participate in the verification of the effective compliance with these policies, processes and procedures by the MSI, as well as process maturity assessments.	Y	
8	Integrate Supplier's Process with the Service Management Manual Processes of the MSI, other Service Tower Suppliers, Customers, and authorized Third Party Vendors, where the processes interact. In cooperation with the MSI, Supplier is required to follow <u>SMM 4.1.6 Continual Improvement</u> which shall include contributing to a quarterly Single process compliance assessment & Continual Service Improvement Register (CSIR) entries with Action Plans and report progress towards closure of the Supplier's assigned actions.	Y	
9	Participate in the MSI Governance framework, described in <b>Exhibit 1.2 (Governance)</b>	Y	

10	Comply with VITA Rules for all Commonwealth data and all systems that contain Commonwealth data and metadata.	Y	
11	Conform to changes to VITA Rules for all Commonwealth data and all systems that contain Commonwealth data and metadata.	Y	
12	Support the periodic audit by Third-Parties as directed by the MSI, VITA or Customers.	Y	
13	Supplier will respond to and participate in VITA Joint Operations Center activities 24x7x365, As it relates to issues or interdependencies associated with service delivery from the Supplier.	Y	
14	Supplier will respond to Priority 1 incidents before and after Business Hours 0700-1900 hours.	Y	
15	Provide 24x7x365 operations, including staffing Supplier Personnel to provide 24x7x365	Y	
<b>2.1 GENERAL</b>			
<i>Supplier's responsibilities include:</i>			
1	As per <u>SMM 4.1.2.4 Service Portfolio Management</u> , among others, supplier will onboard their services with VITA, then manage their lifecycle. Service Portfolio Management (SVP) is to allow the Virginia IT Agency (VITA) to offer the right mix of services to balance the Commonwealth's investment in IT with the ability to meet or exceed the desires of		
2	Perform Project Management as directed by the MSI in <u>SMM 4.1.1.2 Project Portfolio Management</u> , to include but not limited to Requests for Services solution implementation, and for technology Refresh activities. Project Management thus includes planning, coordination with stakeholders, managing execution and conducting communications to stakeholders.	Y	
3	Provide and describe the capability for disentanglement and retention of any Intellectual Property owned by the Commonwealth (i.e., any Cloud capability established on behalf of the Commonwealth becomes property of the Commonwealth at the end of the contract).	Y	
4	Ensure that the environment is in compliance with VITA Rules: <a href="https://www.vita.virginia.gov/policy--governance/governance/vita-rules/">https://www.vita.virginia.gov/policy--governance/governance/vita-rules/</a>	Y	
5	Work with the MSI to schedule and define maintenance windows. <To be included in the KSE Change Management Schedules table for tracking and validation for change management	Y	
6	Manage Supplier relationships and provide a technical interface to MSI, VITA, VITA Customers, other Service Tower Suppliers (STS) and Third-Party Vendors.	Y	
<b>2.2 Engineering and Architecture</b>			
<i>Supplier's responsibilities include:</i>			
1	Introducing and integrating new technologies into existing Cloud environments.	Y	
2	As per SMM 4.1.2.1 Strategy Generation and Planning, participate in strategic technology planning reviews to discuss emerging technologies, strategy exceptions, and performing assessments related to MCS scope.	Y	
3	Maintain a program for the purpose of research and development, utilization, and innovation. These research and development resources shall provide VITA and VITA Customers with future-focused ideas and methodologies for development, utilization, and innovation on a quarterly	Y	
4	Prepare testing and implementation schedules for new technologies based on specific quarterly customer surveys.	Y	
<b>2.3 Service Management Systems</b>			
<i>Supplier is required to use or integrate, through e-bonding or another preapproved integration method, with systems provided by the MSI (i.e., Incident Management System, Change Management System, Configuration Management System and Configuration Management Database (CMDB), etc.). These systems and any systems Supplier provides that integrate with the MSI systems are collectively referred to herein as Service Management Systems (SMS). Exhibit 4.7 (Software Assets) defines the specific MSI toolset</i>			

1	The list below describes the purpose, as defined by VITA, to guide the MSI in providing the SMS, of which the Service Tower Suppliers will be Users and providers of management information. Not all tools below will be applicable to MCS scope or integration and are provided for environmental awareness to the benefit of understanding interactions. Service Management Systems employed in VITA's managed environment are as follows:		
1.1	IT Information Portal: Provide an integrated Portal which provides access and customizable views for the data processed in the Service Management Systems. Displays service measurements as per section 6.3 of this document, including overall program measures and other reports which include, but are not limited to those in <b>Exhibit 3.0 (Reporting and Service Level Management)</b> . Provide dashboard that is customizable by each User.	Y	
1.2	Cloud Broker Technology Integration System: See section <b>2.4 (Cloud Broker Technology Integrator)</b> below.	Y	
1.3	Data Warehouse System: Provide a mechanism to collect data from all Service Management Systems and provide access to the Customers for report generation, with ability to save queries by Customer and individual.		
1.4	Billing, Chargeback and Utilization Tracking System: Provide a mechanism for billing VITA for Services across all Service Tower Suppliers and enable VITA to establish overhead charges and provide billing to Customers.	Y	
1.5	Service Portfolio Database: Provide database of all Services including those under development, in operations, or in process of retirement.	Y	
1.6	Service Catalog and Request Management System(s): Provide a mechanism for Customers to view and order and track Standard Service and Solution Requests/Proposals.	Y	
1.7	Asset Management System: Provide a mechanism for Customers to track all assets.	Y	
1.8	Service Level Management and Reporting System: Provide a system that tracks current and historic Service Levels and the current and historic performance of the Supplier and Service Tower Suppliers. Provide a method for Customers to view and generate reports for current and previous Service Level metrics.	Y	
1.9	Security Clearance System: Provide a mechanism to manage, validate and allow Customers and Users to view the security clearance check status for all individuals providing Services under the MSI and STS.		
1.10	Document Data Store: Provide a mechanism for the common storage of artifacts and data related to projects and program management.	Y	
1.11	Change Management System: Provide a mechanism to track and facilitate the Change Management process.	Y	
1.12	Project Portfolio Management and Project Management Reporting System: Provide the mechanism to track and report the portfolio of projects and programs associated with the ITISP. The system should enable reporting of status, schedules, task assignments, issues and	Y	
1.13	Incident Management System : Provide a mechanism for the tracking and managing Incidents.	Y	
1.14	Knowledge Database: Provide a mechanism for User self-help.	Y	
1.15	Event Management and Correlation System: Provide a mechanism for designated Users to establish alerts and notifications for status changes within any Service Management Systems.	Y	
1.16	Problem Management System and Known Error Database: Provide a mechanism to collect previous errors and resolutions which are accessible by MSI, STS, VITA, Third Party Suppliers and designated Users.	Y	
1.17	Software License Management System: Provide a mechanism to track Enterprise (VITA owned) software license and subscriptions used across all managed Equipment assets.	Y	
1.18	Risk Management System: Provide a mechanism to identify, track, analyze, report and demonstrate remediation of identified risks as part of Risk Management.	Y	
1.19	Information Security Management System (ISMS): Provide an Information Security Management System (ISMS) to maintain the policies, processes, standards, guidelines and tools to support Customers in achieving their Information Security Management objectives.	Y	
1.20	Service Desk Telephony: Provides a contact center system to handle MSI Service Desk contacts via telephone.		

1.21	IT Infrastructure Monitoring System: Provide system that will monitor all assets, providing real-time status (e.g., software versions, patch levels, uptime, hardware performance). (EVENT MANAGEMENT)	Y	
1.22	Identity and Access Management System: Provide system that will allow for identity and access management.	Y	
1.23	Service Continuity Management System: Provide system that will allow MSI to coordinate all Service Tower Service Continuity Management (including planning and testing).	Y	
1.24	Remote administration system: Provide tools and staff to remote into a User's PC to improve first call resolution and reduce mean time to resolution.		
1.25	Capacity Management System: Provide system that will support capacity management process		
2	<i>For all Service Management Systems, in collaboration with and coordinated through the MSI, Supplier responsibilities include:</i>		
2.1	Compliance with VITA Rules (e.g., Security Standards, Federal and Commonwealth mandates, records retention policies).	Y	
2.2	Utilize the Service Management System provided by the MSI to meet the objectives for the Service Management Manual Processes.	Y	
2.3	Participate in the integration of the MSI's Service Management Systems with the other systems used by Supplier to meet the objectives of the Service Management Manual Processes.	Y	
2.4	Provide all data to the MSI for collection or archive in a format that can be integrated in the Data Warehouse System.	Y	
2.5	Limit access to the Supplier's systems to the agreed levels (e.g., by business unit) for the type of Users who require access to the system.	Y	
2.6	Ensure all designated Supplier Personnel and authorized Third-Party Vendors are trained by the MSI in the use of the MSI's Service Management Systems, and trained by the Supplier in the use of the Supplier's systems.	Y	
2.7	Support activities to transfer legacy data ensuring that historic data is maintained.	Y	
2.8	Support efforts to verify the Service Management System contents and correctness of the information contained therein by MSI, Customers, and other designated Third-Parties (e.g., auditing organizations). The Supplier is required to contribute to the MSI's production of a set of actions in the Continual Service Improvements Register for modifications to the systems during and after the Transition plan, and a quarterly release schedule indicating scope, priorities, and schedule performance regarding achieving the improvements	Y	
2.9	Secure systems that integrate to the MSI's Service Management Systems and any supporting database(s) such that commonwealth data is clearly separated from the data of all other customers of Supplier and the customers of Supplier's Subcontractors or other vendors.	Y	
2.10	Where Supplier chooses to host those systems outside of a VITA authorized and approved Data Center or a Customer Data Center, Supplier will provision and maintain all necessary Connectivity into the VITA authorized and approved Data Center the Customer Data Center and manage that Connectivity to meet the MSI designated performance standards.	Y	
<b>2.4 Cloud Broker Technology Integrator</b>			
	<i>The MSI is deploying a Cloud Broker Technology Integrator (CBTI) services platform which will act as the primary interface through which customers will interact. Customers shall not have access to an MCS's CMP, unless approved by VITA.</i>  <i>Industry term for CBTI is Cloud Management Platform (CMP).</i>  <i>The Supplier's responsibilities include:</i>		
1	Integration with the MSI's CBTI. More information on the MSI's CBTI is available in <b>EO App M (CloudScend Overview)</b> .	Y	
2	Enable Agency Users to frictionlessly move workloads across CSP tenants in coordination with the MSI's CBTI.	Y	

Ref #	Requirement	Comply (Y/N)	Supplier Response
	<b>3.0 Enterprise Architecture</b>		
	<b>3.1 General Architecture Requirements</b>		
	<i>The supplier's responsibilities include:</i>		
1	Meet the following five essential NIST cloud characteristics:	Y	
1.1	On-demand self-service - a consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.	Y	
1.2	Broad network access - capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).	Y	
1.3	Resource pooling - the provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, software licenses and	Y	
1.4	Rapid elasticity - capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.	Y	
1.5	Measured service - cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.	Y	
2	Document how the deployment models for Supplier's services comply with COV cloud framework characteristics.  <a href="https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/pses/ndf/Cloud_Based_Hosting_Topic_Report_FINAL.pdf">https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/pses/ndf/Cloud_Based_Hosting_Topic_Report_FINAL.pdf</a>	Y	
3	Document providing how they construct services so that agencies/customers do not pay for features that they do not need.	Y	
4	Only use Approved versions of the technologies covered within the COV Technology Roadmaps.  <a href="https://www.vita.virginia.gov/policy-governance/architecture/cov-technology-roadmaps/">https://www.vita.virginia.gov/policy-governance/architecture/cov-technology-roadmaps/</a>	Y	
5	For IT solutions and technologies that are not covered within COV Technology Roadmaps suppliers shall only use versions or models of IT solutions and technologies that are current (N and N-1) and have vendor or equivalent support.  Note 1: support is defined as a minimum of having available and deployable security patching for IT software  Note 2: it is not allowed to utilize an IT solution or technology that requires an unsupported or N-2 or older technology to work.  Example: an IT management utility that only works with a EOL database or N-2 operating system	Y	
6	IT solutions and services as well as everything supporting supplier provided or managed technologies, IT solutions, and services shall comply with VITA Rules for all supplier provided and managed technologies.	Y	

7	A documented lifecycle including information on currency, general availability, and support (end of service life and end of support) for all supplier provided or managed IT solutions and technologies.	Y	
8	Document all versions of software that their services consume or provide. This includes all software that the service providers use to host, develop, support, test, and deploy their IT solutions (operating systems, languages, databases, editors, etc.)  Note: This requirement does not apply to SaaS (addressed by ECOS process)	Y	
9	Produce and maintain defined and VITA-approved baselines for all supported technologies for all IT solution and technologies provided or managed by the supplier. The baseline documentation shall include:  Note: Examples of baselines are Center for Internet Security (CIS) and Department of Defense (DoD) Security Technical Implementation Guides (STIGs)	Y	
9.1	All of the security control settings and configurations available to be configured for the system component the baseline	Y	
9.2	The description of the security control settings and configurations and what they do	Y	
9.3	The baseline settings from an industry recognized framework (if available) or an explanation of why one is not available for that particular system component	Y	
9.4	The recommendation from the supplier if the security control setting or configuration will be enabled or disabled	Y	
9.5	An explanation or rational statement for each recommendation	Y	
9.6	An explanation if there is a difference between the supplier recommendation and the industry recognized framework	Y	
10	Follow the COV baseline process for all supported IT solutions and technologies and shall review baseline documentation at least annually and update as required.	Y	
11	Per applicable SMMs, including but not limited to <u>SMM 4.1.2.2 IT Technology Planning</u> and <u>SMM 4.1.4.4 Service Asset and Configuration Management</u> , and <u>SMM 4.1.4.1 Change Management</u> , the Supplier shall track the lifecycle of all Software and Hardware used to deliver Services in the <u>Service Management System (SMS) provided by the MSI</u> .	Y	
12	Per applicable SMMs, including but not limited to <u>SMM 4.1.2.2 IT Technology Planning</u> , the Supplier shall generate technology roadmaps to include Refresh schedule, Software Upgrades, and new technology to ensure Supplier service offerings stay current.	Y	
13	Perform Equipment Maintenance, Refreshes, Installations and Retirement in accordance with the Refresh and Currency Plans and schedules established by MSI, VITA and ITISP Governance as per <u>SMM 4.1.1.4 Ongoing Programs</u> .	Y	
<b>3.1.1 Design/Architecture Requirements</b>			
<i>The supplier's responsibilities include:</i>			
1	Per <u>SMM 4.1.2 Service Strategy</u> and <u>SMM 4.1.3 Service Design</u> , coordinate all Architecture, design, strategy, and planning activities with MSI, VITA, and VITA Customers (including business units and Project managers).	Y	
2	That all new, changes, or updates to IT solutions go through a formal architecture review process (MSI HARP process.) coordinated by the MSI. More information on the MSI HARP process is available in the following Environment overview documents:	Y	
2.1	<b>EO Appendix Ia (Architecture Review Charter)</b>	Y	
2.2	<b>EO Appendix Ib (Enterprise Services Architecture Overview Document Template)</b>	Y	
2.3	<b>EO Appendix Ic (New Architecture Review Process)</b>	Y	
2.4	<b>EO Appendix Id (Solution Design Management Service Management Manual (HARP))</b>	Y	
3	Document the solution using a VITA approved template provided by the MSI per <u>SMM 4.1.3.1 Solution Design</u> .	Y	
4	Besides the template information to be completed, the Architecture team shall ensure Documentation is provided for:	Y	
4.1	Traceability of all Resource Units (RU) to the Architectural Overview Document (AOD)	Y	
4.2	A Requirements Traceability Matrix (RTM) of Supplier contract <b>Exhibit 2.1 (Description of Services - Managed Public Cloud Services)</b> Service Requirements	Y	

5	All new IT solutions and technologies utilized by supplier or provided to COV customers shall appear on the supplier's high-level service model diagram. This diagram shall include all technology and service components.  Note: This applies to technology components not specific devices (Servers vs. a particular Dell	Y	
6	All new and changes to supplier provided or managed IT solutions and technologies shall be documented at three levels within an Architecture Overview Document (AOD):  Note: The three levels described below may be within separate sections of the same AOD	Y	
6.1	High-level section (HL) - required to be approved prior to starting the project to build the	Y	
6.2	Detailed Design section (DD) - contains the information needed to build or rebuild the system and needs to be completed prior to service going live. It contains not only the system configuration, but also the configurations from any other suppliers that they need to do to bring your system	Y	
6.3	As built (AB) - contains any variances from the Detailed Design and their configurations. It needs to be completed prior to project closeout.	Y	
7	An indication where that component is documented within the supplier's high-level service model diagram for all supplier provided or managed IT solutions or technologies.	Y	
8	All new and changes to supplier provided or managed IT solutions and technologies shall go through a formal VITA approved architecture review process utilizing a template for high-level, detail-level, and as-built designs. The designs need to cover the following architectural viewpoints:	Y	
8.1	Context – describes the relationships, dependencies, and interactions between the system and its environment (the people, systems, and external entities with which it interacts)	Y	
8.2	Functional – describes the system's runtime elements, their responsibilities, interfaces, and primary interactions	Y	
8.3	Information – describes the way that the architecture stores, manipulates, manages, and distributes information	Y	
8.4	Concurrency – describes the concurrency structure of the system and maps functional elements to concurrency units to clearly identify the parts of the system that can execute concurrently and how this is coordinated and controlled	Y	
8.5	Development – describes the architecture that supports the software development process	Y	
8.6	Deployment – describes the environment into which the system will be deployed and the dependencies that the system has on elements of it	Y	
8.7	Operational – describes how the system will be operated, administered, and supported when it is running in its production environment	Y	
9	Provide design documents that shall also address the following architectural perspectives cut across all the views specified in the above requirement:  Reference: Viewpoints, perspectives, and their definitions are from, Software Systems Architecture, 2nd Edition, Nick Rozanski and Foin Woods	Y	
9.1	Security – the ability of the system to reliably control, monitor, and audit who can perform what actions on which resources and the ability to detect and recover from security breaches	Y	
9.2	Performance and Scalability – the ability of the system to predictably execute within its mandated performance role and to handle increased processing volumes in the future if required	Y	
9.3	Availability and Resilience – the ability of the system to be fully or partly operational as and when required and to effectively handle failures that could affect system availability	Y	
9.4	Accessibility – the ability of the system to be used by people with disabilities	Y	
9.5	Development Resource – the ability of the system to be designed, built, deployed, and operated within known constraints related to people, budget, time, and materials	Y	
9.6	Usability – the ease with which people who interact with the system can work effectively	Y	
9.7	Regulation – the ability of the system to conform to local and international laws, quasi-legal regulations, policies, and other rules and standards	Y	
9.8	Evolution – the ability to be flexible in the face of the inevitable change that all systems experience after deployment, balanced against the costs of providing such flexibility	Y	
10	Provide Architecture that Supports service continuity where required.	Y	
11	Provide an engineered solution to allow for choices in hosted geographic data locations to optimize network throughput and remove risk of latency due to Network constraints.	Y	

12	Isolate VITA environments as required to meet VITA Rules.	Y	
13	Isolate VITA Customer environments as required to meet VITA Rules.	Y	
14	Provide a configuration which optimizes the solution to meet a high availability outcome of the environment as dictated by required business outcomes.	Y	
15	Maintain and update the environment and supporting Documentation for their solution's full footprint at least annually. Supplier will continuously leverage new tools and technologies to improve VITA and VITA Customer business processes and performance in accordance with ITISP Governance processes and procedures as defined in the SMM with prior approval obtained by	Y	
<b>3.1.2 Availability / Performance Requirements</b>			
<i>The supplier's responsibilities include:</i>			
1	Ensure Network Performance Simulation Modeling and Application Emulation (NPMAE) is performed, and reported to VITA through the MSI for all proposed Supplier IT solutions that can Impact the Wide Area Network (WAN).	Y	
2	Have defined expected and quarterly measured Mean Time Between Failure (MTBF) metrics for supplier provided and managed IT solutions and technologies	Y	
3	The Solution's IT Components Supporting COV IT services shall have better Availability than the SLAs for the services that consume those components.	Y	
4	Per SMM 4.1.3.4 Availability Management, provide monitoring consistent with Service Level requirements and reporting of System performance, utilization, and efficiency in accordance with	Y	
5	Establish System tuning and performance processes where necessary and Upgrade and tune Services Infrastructure to meet capacity changes in accordance with the SMM, including but not limited to SMM 4.1.3.4 Availability Management and SMM 4.1.3.6 Capacity Management.	Y	
6	Establish and maintain event management mechanisms which apply to the services, as per SMM 4.1.5.3 Event Management.	Y	
7	Establish and maintain monitoring Systems for their solutions, which apply to platforms and	Y	
8	Monitor all phases of their solution's Systems performance.	Y	
9	For all COV IT services, the Supplier shall have SLA's or key measures for Availability and	Y	
10	Provide appropriate real-time and analysis of historical performance data obtained through monitoring of all phases of their solution's Systems performance.	Y	
11	Conduct System performance testing of their entire solution to include in reporting.	Y	
12	Provide Systems performance review report(s), including recommendations and advice, after conducting required System performance testing of their solutions.	Y	
<b>3.1.3 Capacity and Performance Requirements</b>			
<i>Supplier's responsibilities include:</i>			
1	Per SMM 4.1.3.6 Capacity Management, perform strategic, tactical, and operational procedures.	Y	
2	Perform Infrastructure or Platform Upgrades of their solutions to provide effective capacity to meet VITA and VITA customer needs. Coordinate their Projects with VITA, VITA business partners, VITA Customers, Third Party vendors, and other vendors as appropriate to manage Infrastructure	Y	
3	Per SMM 4.1.6.3 Service Measurement, perform activities required for optimizing performance of their solutions to reduce costs.	Y	
4	Per SMM 4.1.6.3 Service Measurement, perform activities required for optimizing performance of their solutions to improve Service Levels.	Y	
5	Identify estimated bandwidth usage per Application. In addition to requirements stipulated in SMM's, the following shall be maintained in the Archer application for each Solution Application:	Y	
5.1	Number of average concurrent Users on the Application (concurrent is defined as Users transmitting or receiving application data at the same time)	Y	
5.2	Amount of bandwidth required for each concurrent User	Y	
5.3	Amount of total Users for each Application	Y	
5.4	Number of concurrent Users during highest Application usage (i.e. visitors during tax season, hurricanes, document submissions, etc.)	Y	
5.5	The Application throughput estimate (how much network traffic can be processed at once)	Y	
<b>3.1.4 Continuity Requirements</b>			
<i>The supplier's responsibilities include:</i>			
1	Support service continuity in accordance with SMM 4.1.3.5 IT Service Continuity Management.	Y	
2	Recommend service recovery point objectives (RPO) and recovery time objectives (RTO) for their	Y	
3.0 Enterprise Architecture	services, on demand, for VITA to review and approve.	Y	

3	Design, configure and deploy, either supplier provided or managed IT solutions and technologies, which meet VITA defined service recovery point objectives (RPO) and recovery time objectives	Y	
4	The Solution shall meet defined service Recovery Time Objectives (RTO) as stipulated by agencies and/or Customers.	Y	
5	Test and determine that all their services are free of defects and compliant with VITA Rules.	Y	
6	Ensure that any vendors and VITA Customer approved maintenance providers used by the supplier, properly maintain all Hardware and Software.	Y	
7	The Solution shall have a Technical Recovery Guide for all of its Application Components and Configurations.	Y	
8	The Solution shall comply with the Virginia Public Records Act, Code of Virginia 42.1-76-42.1-91, which requires uniform management and preservation of public records in Commonwealth government agencies.	Y	
9	The Solution shall consider and address the Impact on Commonwealth Data of both System outages and data corruption in meeting established RPOs.	Y	
10	The Solution shall comply with COV ESA Data Availability requirements for all Commonwealth Data.  <a href="https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/psgs/pdf/EA-Solution-Data-">https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/psgs/pdf/EA-Solution-Data-</a>	Y	
11	Ensure that the additional sites used for data replication and backup provide geo-diversity,	Y	
11.1	Data locations should be at least 400 miles away from each other	Y	
11.2	Data locations should be where the risk of natural disasters are acceptable to the COV. Natural disasters include but are not limited to forest fires, lightning storms, tornadoes, hurricanes, earthquakes and floods. Additionally, the Site needs to be located within the continental United	Y	
11.3	Data locations should be in an area where the possibility of man-made disaster is low. Man-made disasters include but are not limited to plane crashes, riots, explosions, and fires. The Site should not be adjacent to airports, prisons, freeways, stadiums, refineries, pipelines, tank farms.	Y	
12	The Solution shall not rely solely on replication as a technique to address data corruption.	Y	
13	The Solution shall provide Customers the ability to perform backups and restores of their Commonwealth Data.	Y	
14	The Solution shall test for data corruption and notify the Customer when corruption occurs.	Y	
<b>3.1.5 Technology Requirements</b>			
<i>The Supplier's responsibilities include:</i>			
1	Use components in solutions whose currency lifecycle phase includes update-level support. Do not use components that do not meet VITA Rules for currency.	Y	
2	Provide Support for heterogeneous platforms in various geographic locations within the Unites	Y	
3	Provide Support for heterogeneous platforms that interface with Cloud or premise-based	Y	
<b>3.1.6 Integration/Interoperability Requirements</b>			
<i>The Supplier's responsibilities include:</i>			
1	Ensure the Solution integrates into all System logging with VITA and/or other Service Tower	Y	
2	Ensure the Solution integrates into all application logging with VITA and/or other Service Tower	Y	
3	Ensure the Solution complies with COV Event Log Management requirements.  <a href="https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/ea/pdf/Event-Log-">https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/ea/pdf/Event-Log-</a>	Y	
4	Ensure the Solution integrates monitoring consoles with MSI to allow MSI, VITA and Customers the ability to establish notifications.	Y	
5	Ensure the Solution integrates monitoring consoles with MSI to allow MSI and VITA Customers the ability to set notification thresholds.	Y	
6	Ensure the Solution is thoroughly tested for integration and meets VITA requirements.	Y	
7	Ensure the Solution is thoroughly tested for interoperability and meets VITA requirements.	Y	
8	Ensure the Solution enables all Services to interact regardless of where and how they are hosted.	Y	
9	Ensure the Solution Components integrate across all supported form factors, such that they seamlessly interact with each other while leveraging their native capabilities in a way where they do not require additional Configuration or administration.	Y	
10	Ensure the Solution supports the creation and update of all data types covered by VITA Rules.	Y	

A	B	C	D
1	<b>VA-240920-NTT: Managed Public Cloud Services</b>		
2			
3	<b>Ref # Requirement</b>	<b>Comply (Y/N)</b>	<b>Supplier Response</b>
4	<b>4.0 Security Requirements</b>		
5	<b>4.1 General Security Requirements</b>		
6	<i>The Supplier's responsibilities include:</i>		
1	Ensure the Solution shall comply with Commonwealth security policies and standards, VITA Rules, <u>SMM 4.1.3.7 Security Management</u> , <u>SMM 4.1.3.8 Risk Management</u> (and among other SMMs), and all Customers' individual Information Security Policies and applicable Federal standards (e.g., FedRAMP moderate or high, SEC525, CJIS, FISMA, PCI, ISO27001, FERPA, FTI (IRS PUB-1075), SSA, HIPAA-HITECH and any updates to these listed standards.)	Y	
2	Grant access to specified systems, services, and/or other technologies shall be granted to the Chief Information Officer, the Chief Information Security Officer for the Commonwealth of Virginia, or an identified designee with credentials upon request.	Y	
3	Provide informed advice on Security policy, standards (including national security, international, customer and industry standards), practices, solutions and technologies, and threats.	Y	
4	Implement Security management processes, procedures and controls with other service providers to address interdependencies, use of tools and workflows required to operate integrated Security Management across the Services.	Y	
5	Provide a description of all software which utilizes the Cloud in order for VITA to perform a COV Ramp assessment. Please provide all information in <b>Exhibit 2.3.1 (Solution - Managed Public Cloud Services)</b> . Review COV Ramp summary at <a href="https://www.vita.virginia.gov/cov-ramp/">https://www.vita.virginia.gov/cov-ramp/</a>	Y	
6	Ensure the Solution is supported and maintained by US Citizens or those legally allowed to work in the US.	Y	
7	Ensure the Solution is housed within a container reserved for the exclusive use of the Commonwealth. All storage, backups, and replication, must remain within the US. See PE-18-COV.	Y	
8	Ensure the Solution will support multiple levels of administration to allow Configuration changes at the Enterprise and Agency	Y	
9	Ensure all User activity and System administration activity is logged.	Y	
10	Ensure all logged Events are provided to the VITA Managed Security Service Provider for analysis in a VITA approved format utilizing a VITA approved automated method. Ensure VITA Agencies logged events are provide for Agencies view and use.	Y	
11	Ensure that all Commonwealth Data remains in the United States and all Sensitive Data remains encrypted at rest and while	Y	
12	Ensure that the Commonwealth retains exclusive control and ownership of all encryption keys used in the solution in accordance with VITA Rules.	Y	
13	Ensure that encryption will allow for Time-based revocation of access/encryption keys based on the schedule defined by VITA and VTIA Customers.	Y	
14	Ensure that Encryption will allow for User-based revocation of access/encryption keys.	Y	
15	Ensure that all data associated with the Solution is encrypted in transit and at rest between services and Systems.	Y	
16	Ensure that all encryption mechanisms in use by the solution is compliant with VITA Rules.	Y	
17	Establish and maintain mechanisms and notifications to safeguard against the unauthorized access, destruction, loss or alteration of Customer's data per VITA Standards.	Y	
18	Utilize controls and processes such that the Services are compliant with all VITA Rules for the processing, Storage and transmission of information based on its classification and Impact categorization and ensure that Customers are able to gain assurance and evidence that such compliance is being maintained upon request.	Y	
19	Disable or delete accounts in accordance with VITA Rules for standard expiration (e.g., 90 days without use) or promptly as	Y	
20	Evaluate existing VITA tools and environment current state of malware prevention, unauthorized code prevention, IDS/IPS, Phishing, Spamming, File Integrity Monitoring, and denial of service Software and tools. Determine approach and solution as applies to the Suppliers implementation, obtain VITA approval of plan, then install, update, operate, and maintain as applicable to comply with VITA Rules or Customer-specific rules and in accordance with industry best practices on all Equipment used to deliver or support the Services.	Y	
21	Maintain subscription to services that proactively announce vulnerability, Patch, and pattern Updates and redeployment of updated systems.	Y	
22	Install available Updates, in accordance with Change Management, to malicious-prevention Software and services as needed or as directed by VITA, within the timeframes specified by relevant Third Parties, vendors, or industry experts – except as otherwise approved by VITA.	Y	
23	Ensure that Solution will integrate into the VITA CASB and Logging Services.	Y	
24	Ensure that Solution will log all access attempts (successful / unsuccessful) by an administrative User or by personnel supporting the solution from any service provider associated with the Solution and that the logs are automatically forwarded to the VITA Managed Security Services Provider for analysis.	Y	
25	Ensure that Solution will log all actions taken by an administrative User or by personnel supporting the solution from any service provider associated with the Solution and that the logs are automatically forwarded to the VITA Managed Security Services Provider for analysis.	Y	

	A	B	C	D
26 32		Ensure that no personnel supporting or administrating the Solution can alter or delete any log associated with the support or operation of the Solution.	Y	
27 33		Ensure that no personnel supporting or administrating the Solution can alter or stop any logging service associated with the support or operation of the Solution.	Y	
28 34		Ensure that any service migration between platforms will ensure zero residual data on the originating platform once the Service is migrated and provide evidence of data removal with a certificate of destruction in accordance with VITA Rules.	Y	
29 35		Ensure there are no shared accounts and that each account (human or service) is owned/has a responsible party assigned	Y	
30 36		<i>In the space below, suppliers shall list any additional security standards which they can comply with if requested by customers to meet their needs. Suppliers may add rows below should additional space be needed.</i>		
37	30.1	NIST RMF/CSF	Y	
38	30.2	Criminal Justice Information System (CJIS)	Y	
39	30.3	Social Security Administration (SSA)	Y	
40		Federal Information System Management Act (FISMA)	Y	
41		ISO 270001	Y	
42		FERPA	Y	
43		FIT (IRS Pub 1075)	Y	
44		HIPAA-HITECH	Y	
45		MARS-E 2.0	Y	
46		ISO 22301 - Business Continuity Management	Y	
47		ISO 31000 - Risk Management	Y	
48		ISO 20000-1 - IT Service Management	Y	
49		SOC 2 Type II - Service Organization Control for Cloud and Data Center Providers	Y	
50		CIS Controls - Center for Internet Security Controls	Y	
51		GLBA - Gramm-Leach-Bliley Act for financial institutions	Y	
52		Sarbanes-Oxley Act (SOX) - For corporate governance and financial disclosure	Y	
53		PCI-DSS - Payment Card Industry Data Security Standard for payment card transactions	Y	
54		CMMC - Cybersecurity Maturity Model Certification	Y	
55		NERC CIP - North American Electric Reliability Corporation Critical Infrastructure Protection	Y	
56		GxP - Good Practice guidelines for industries like pharmaceuticals, food, and medical devices	Y	
57		OWASP Top 10 - Open Web Application Security Project guidelines for web application security	Y	
58		COPPA - Children's Online Privacy Protection Act	Y	
59		SCA - Stored Communications Act	Y	
60		ECPA - Electronic Communications Privacy Act	Y	
61		<b>4.1.1 Incident Response Security Requirements</b>		
62		<i>The Supplier's responsibilities include:</i>		
63	1	Participate in the Incident response process as required by VITA and its Customers or as requested by the MSI.	Y	
64	2	Submit and receive approval for an Incident Response Plan for the Solution from VITA on an annual basis.	Y	
65	3	Provide input into the Integrated Incident Response Plan used by VITA and the MSI to conduct Incident response as required by VITA Rules and the SMM 4.1.5.7 Security Incident Management.	Y	
66	4	Respond to and Resolve malware, unauthorized content, hacking, phishing, denial of service, and other Incidents as defined by VITA and the MSS. Upon detection of malware or unauthorized content, take immediate steps to notify VITA and the	Y	
67	5	Once the Incident is declared, work with the MSI, MSS, and VITA to assess the scope of damage.	Y	
68	6	Report status of the Incident and mitigation activities to VITA once every 24-hours or more frequently as required by VITA until the Incident is Resolved.	Y	
69	7	Arrest the spread and progressive damage from malware or unauthorized code in accordance with the VITA approved Incident response plan.	Y	
70	8	Eradicate malware or unauthorized code in accordance with the VITA approved Incident response plan.	Y	
71	9	Restore all data and Software to its last-known operational state in accordance with the VITA approved Incident response plan. Provide a Root Cause Analysis to prevent/mitigate this type of incident.	Y	
72	10	Provide proactive alerts to VITA, the MSI, or Customers as appropriate relative to current code threats either specific to VITA's environment, encountered in Supplier's environment, or based on industry information.	Y	
73	11	Provide expertise , including forensic, in the Event of a major computer malware, outbreak, phishing, hacking, denial of service, or similar Event so VITA's and Customers' performance does not degrade because of an unavailability of Supplier	Y	
74	12	Respond to Security Incidents or emerging Security requirements (which may arise as a result of changing Security standards, threats or industry practices) under direction from Customers. Based on versions of OS/Database/Application servers, provide VITA notification and plan to remediate published CVE or vulnerabilities.	Y	

	A	B	C	D
75	13	Provide data feeds or Reports to VITA's Security Incident and Event correlation Systems for purposes of deep analytics in accordance with VITA Rules and SMM 4.1.3.7 Security Management in order to support VITA's analysis as requested.	Y	
76		<b>4.1.2 Security Integration</b>		
77		<i>The Supplier's responsibilities include:</i>		
78	1	Perform or Integrate with current and future COV Enterprise Cyber Security services, including those of which are managed by VITA or other Service Tower Suppliers. A list containing a portion of these integration points are provided in various Environment Overview documents such as <b>EO App L (Managed Security Tools and Integration Methodologies)</b> . This includes	Y	
79	1.1	Event Log Management services (including incident management)	Y	
80	1.2	Event Management System (SIEM service)	Y	
81	1.3	Threat Intelligence Platform (TIP) service	Y	
82	1.4	Security Orchestration, Automation, and Response (SOAR) service	Y	
83	1.5	Managed Detection and Response (cyber analytics) Services	Y	
84	1.6	Single Sign-on	Y	
85	1.7	Identity Access Management Services	Y	
86	1.8	Identity Governance services	Y	
87	1.9	Privileged Access Management (PAM)	Y	
88	1.10	Directory Services	Y	
89	1.11	Patch and software deployment services	Y	
90	1.12	Cloud Access Security Broker service (CASB)	Y	
91	1.13	Managed Firewall Services	Y	
92	1.14	Managed Network Intrusion Prevention (NIPS) Cloud Service	Y	
93	1.15	Remote User Access Service	Y	
94	1.16	Remote Access Network Service	Y	
95	1.17	Web Application Firewall (WAF)	Y	
96	1.18	Compliance Testing Network Service (network access control (NAC))	Y	
97	1.19	Web Gateway Security Service	Y	
98	1.20	Endpoint Security Services	Y	
99	1.21	Application Security Service	Y	
100	1.22	Data Loss Prevention	Y	
101	1.23	Vulnerability Management Service	Y	
102	1.24	Enterprise Network Monitoring Service	Y	
103	1.25	Native CSP network and Application security tools (e.g. IP and DNS management)	Y	
104	1.26	Full Packet capture	Y	
105	1.27	SSL Certificate Management	Y	
106	1.28	OS and Antivirus patching/update services	Y	
107	1.29	Key Management	Y	
108	1.30	Other COV security related services	Y	
109	2	Submit and receive approval from VITA of a System Security Plan(s) in accordance with VITA Rules and the <u>SMM 4.1.3.7</u> Security Management.	Y	
110	3	Provide reporting to VITA and VITA Customers that highlights emerging threats and the status of known risks in accordance with VITA Rules and the SMM 4.1.3.8 Risk Management.	Y	
111	4	Initiate Corrective Actions Plan in respect of any potential or actual Security issues or Noncompliance with the procedures in accordance with VITA Rules and the SMM.	Y	
112	5	Participate in the integrated compliance and Security Management service performance plans and Reports for all Service Security requirements to meet VITA and VITA Customer's informational reporting requirements and Service Levels in a regular and timely manner.	Y	
113	6	Integrate with Managed Security Supplier via the MSI to Support Managed Security Services Platform toolsets on the Platform Services.	Y	
114	7	Name, Install, operate, Configure, Support, and manage Security related toolsets in support of the Managed Security Services Platform toolset in accordance VITA Rules and the SMM.	Y	
115	8	Monitor the environment to detect and prevent Intrusions in accordance with the VITA Rules and the SMM.	Y	
116	9	Communicate and report any intrusion detected in the environment in accordance with the SMM.	Y	
117	10	Solution will ensure all Events required by VITA Rules and the SMM be logged and forwarded to the MSS SIEM for review and	Y	
118	11	Solution will provide documented API integration with all VITA and MSS security tools.	Y	
119		<b>4.1.3 Audit and Compliance</b>		
120		<i>The Supplier's responsibilities include:</i>		
121	1	Provide the non-redacted SOC 1 audit results to VITA and VITA Customers at least once every 12-months.	Y	

	A	B	C	D
122	2	Provide the non-redacted SOC 2, Type II audit results to VITA and VITA Customers at least once every 12-months.	Y	
123	3	Provide quarterly updates to Commonwealth Security on remediation steps taken for SOC1 and SOC2 Exceptions.	Y	
124		<b>4.1.4 User Authentication</b>		
125		<i>The Supplier's responsibilities include:</i>		
126	1	Adhere to SMM 4.1.5.6 Access Management.	Y	
127	2	Ensure that Solution will provide single sign-on Functionality.	Y	
128	3	Ensure that Solution authentication process will integrate into COV Directory Service and tools.	Y	
129	4	Ensure that the Solution will federate with the VITA approved single sign-on authority (e.g.; OKTA).	Y	
130	5	Ensure that the Solution will enforce interactive re-authentication at regular intervals as defined by VITA and its Customers.	Y	
131	6	Ensure that the Solution will log and provide audit Events for all authentication attempts.	Y	
132	7	Ensure that all logs are forwarded to a centralized repository of VITA choosing (SIEM).	Y	
133	8	Utilize security clearance and access control processes to administer tools and environments used to support Customer's services for all staff.	Y	
134	9	Ensure that access privileges for Supplier Personnel are promptly removed upon departure from the program in accordance with VITA Rules and the SMM.	Y	
135	10	Perform a semi-annual review of all users and a quarterly review of Admins access.	Y	
136		<b>4.1.5 User Authorization</b>		
137		<i>The Supplier's responsibilities include:</i>		
138	1	Ensure that any required document Storage authentication or authorization is controlled via a centralized policy setting that can be applied at the Enterprise and Agency level.	Y	
139	2	Ensure that the Solution will log and store all User interactions.	Y	
140	3	Ensure that all logs are forwarded to a centralized repository of VITA choosing (SIEM).	Y	
141	4	Ensure that all logs are maintained according to VITA and Customer records retention policy.	Y	
142		<b>4.1.6 Encryption at Rest</b>		
143		<i>The Supplier's responsibilities include:</i>		
144	1	Implement encryption at rest as required by VITA Rules and in accordance with the SMM.	Y	
145	2	Provide the ability to perform a forensic analysis of the encrypted data.	Y	
146	3	Ensure that the Device will be able to be decrypted with the forensic Software to support the forensic analysis. Provide key escrow services.	Y	
147		<b>4.2 List of Tools</b>		
148		<i>The Supplier's responsibilities include:</i>		
149	1	Provide a list of tools in <b>Exhibit 2.3.1 (Solution - Managed Public Cloud Services)</b> or as an appendix to <b>Exhibit 2.3.1 (Solution - Managed Public Cloud Services)</b> . Include reports from the tools that support the solution, and costs of the tools.		
150		<b>4.3 Security Approach</b>		
151		<i>The Supplier's responsibilities include:</i>		
152	1	Security, compliance, encryption, auditing, and other InfoSec concerns should be addressed deep within the platform via thoughtful implementation of automation and reference architectures.	Y	
153	2	Codify and implement security policies to enforce compliance, and operational best practices across all service provisioning. A "shift left" approach must be used to automate enforcement, ensuring that changes are in compliance without creating a manual review bottleneck.	Y	
154	3	Enforce policies on the types of infrastructure created, how it is used, and what can be created and by who. Appropriate and approved policy as code framework must be adopted to provide compliance and governance without requiring a shift in the overall team workflow.	Y	
155		<b>4.4 Security Management</b>		
156		<i>Security Management will assess that all security risks associated with the delivery of Services are appropriately identified, evaluated, assessed, remediated, and appropriate controls are implemented and maintained. Security Management will be performed in a manner consistent with VITA Rules. Refer to Environment Overview Appendix C: Security environment overview for an overview of the existing environment. The Supplier's responsibilities include:</i>		
157	1	Implement, maintain, and continuously comply with VITA Rules and Security Baseline Configuration Standards as defined in the VITA approved hardening guides, SMM, or as defined by specific Customer security requirements.	Y	
158	2	Utilize the Information Security Management System (ISMS) as provided by the MSI, to maintain the policies, processes, standards, guidelines and tools to support VITA and Customers in achieving their Information Security Management objectives. Additional Supplier's responsibilities shall include but not be limited to:	Y	
159	2.1	Update the ISMS in a timely manner based on Changes to the technical environment.	Y	

	A	B	C	D
160	2.2	Validate the ISMS contents to ensure the accuracy and completeness of the data contained therein on a routine basis, in accordance with the SMM.	Y	
161	3	Understand VITA Rules in detail, to enable informed interactions with the MSI, Customers and End Users, VITA and other Service Tower Suppliers.	Y	
162	4	Assist Customers in the definition of security requirements based upon Business needs and Customer's individual information security policies and Regulatory Requirements, as those needs and policies relate to the Services, and as requested by the	Y	
163	5	Provide informed advice on security policy, standards (including national security, international, customer and industry standards), practices, solutions and technologies, and threats related to the Services.	Y	
164	6	Implement Operating Level Agreements and Security Management processes, procedures and controls across Supplier Services, and the other Service Tower Suppliers to address interdependencies, use of tools and workflows required to operate integrated Security Management across the Services	Y	
165	7	Implement and comply with all VITA Rules and Customers' Individual Information Security Policies, and all security requirements defined for the Managed Environment.	Y	
166	8	Participate in the integrated compliance and Security Management Service performance Plans of Action and Milestones (POAM), and reports for all Service security requirements to meet Customers' informational reporting requirements and Service Levels in a regular and timely manner.	Y	
167	9	Track, expedite and report upon actions raised against plans, reports and Self-Assurance Statements.	Y	
168	10	Escalate security management improvement opportunities, issues, risks, events or any other pertinent security matter identified in accordance with the processes and procedures defined in the SMM.	Y	
169	11	Respond to Security Incidents or emerging security requirements (which may arise as a result of changing security standards, threats or industry practices) under direction from the MSI, and in accordance with the processes and procedures defined in	Y	
170	12	Utilize security clearance and access control processes to administration tools and environments used to support Customer's Services for all staff, in accordance with the processes and procedures defined in the SMM.	Y	
171	13	Ensure that access privileges for Supplier Personnel are promptly removed upon departure from the ITISP.	Y	
172	14	Establish and maintain mechanisms to safeguard against the unauthorized access, destruction, loss or alteration of	Y	
173	15	Implement safeguards that are compliant with Customers' Information Security Policies and Standards and in accordance with the processes and procedures defined in the SMM.	Y	
174	16	Utilize controls and processes such that the integrated Services are compliant with all relevant regulations, policies and standards for the processing, storage and transmission of information based on its classification and impact categorization, and ensure that Customers are able to gain assurance and evidence that such compliance is being maintained upon request	Y	
175	17	Provide reporting to the MSI that highlights emerging threats and the status of known risks.	Y	
176	18	Deploy security processes to enable effective monitoring and reporting of Services and provide data to the MSI from monitoring controls and processes related to emerging threats and known risks.	Y	
177	19	On an on-going basis, check the effectiveness of the security procedures and controls, and compliance with regulations.	Y	
178	20	Initiate corrective actions in respect of any potential or actual security issues or noncompliance with the procedures.	Y	
179	21	Produce a weekly, or in accordance with the SMM, security status report to detail on-going work and actions identified and completed.	Y	
180	22	Monitor and control remote data communication access to Customers' Infrastructure, Software, Equipment, and all other	Y	
181	23	Routinely perform feasibility studies and evaluations for the implementation of new security technologies, based on threat trends, which meet Commonwealth requirements and objectives and report these to MSI and VITA.	Y	
182	24	Develop and maintain System Security Plan (SSP) and actively participate in the SSP approval process. <i>For more information on the System Security Plan, refer to the following Environment overview documents:</i>  · <b><i>Environment Overview Appendix Ja: System Security Plan Template</i></b>  · <b><i>Environment Overview Appendix Ib: Service Management Manual (SSP)</i></b>	Y	
183	<b>4.5 Security Program</b>			
184	<i>Security Program will be an On-Going Program. The Supplier's responsibilities include:</i>			
185	1	Participate in the continuous Security Program, which will comprise the on-going activities that accomplish the goals for security management and coordinate the activities of Customers, Supplier, the MSI, and designated Third-Party Vendors.  Note: The VITA Security Plan and Policy will govern the periodic activities for Security Management conducted by the MSI and Service Tower Suppliers including periodic patching, plans for implementing security measures, security performance monitoring and periodic security assessments and testing	Y	
186	2	Adhere to the comprehensive VITA Security Plan and Policy that defines the security requirements of the ITISP environment and supports the security of Customers' systems, Software and information.	Y	

	A	B	C	D
187	3	Develop, implement and maintain internal standards, processes and procedures which enable compliance with VITA Rules and Customer requirements. Provide the MSI, VITA and Customers access to all standards, processes and procedure	Y	
188	4	Implement and maintain internal security awareness training processes and procedures and provide communications that ensure Supplier Personnel are aware of the security and operational requirements of the program.	Y	
189	<b>4.6 Security Assessments</b>			
190	<i>Supplier's responsibilities include:</i>			
191	1	As defined in the SMM, or requested by VITA or ITISP Governance, participate in a VITA assessment of the Security Program and Services from MSI and Service Tower Suppliers.  Note: Including the monitoring and testing of security programs (e.g., Controlled Penetration Tests), conducting risk assessments and performing Security Design Reviews, of all or any portion of the Services in order to evaluate the Security Program and determine whether the Security Program meets or exceeds the standard of due care	Y	
192	2	Such assessments will evaluate Supplier's abilities and capabilities in maintaining and enhancing security and safety practices and procedures, and may involve monitoring and testing security programs, conducting risk assessments and performing Security Design Reviews.  Note 1: Each assessment will examine network deployment and infrastructure to ensure the proper protection of both the Systems and data while in use, storage, transmission or destruction.  Note 2: At a minimum, each assessment will address potential deployment and infrastructure issues to insure the Availability, integrity, confidentiality and privacy of information and information systems operated by the Service Tower Suppliers, and include all areas as described in the SMM at a minimum (e.g., asset name, owner, risk analysis, controls).  Note 3: Customers, the Auditor of Public Accounts, and other-Third Party Vendors authorized by VITA may conduct security reviews, assessments, forensic analysis or audits (e.g., AICPA's SOC 2, U.S. Internal Revenue Service 1075 audits, or risk assessments following NIST Special Pub 800-30 "Guide for Conducting Risk Assessments") of the Services being provided by the MSI and Service Tower Suppliers.  Note 4: These assessments may include physical security, logical security, processing integrity, continuity of operations,	Y	
193	3	Assess security stance of all new, changed and / or upgraded Hardware, Software, or Services to ensure continued compliance with configuration requirements.	Y	
194	4	Implement any changes, through the Change Management Process documented in the SMM, needed to comply with VITA Rules and Customer requirements, based on results of any and all assessments.	Y	
195	<b>4.7 Security Assessment by Third Parties</b>			
196	<i>Supplier's responsibilities include:</i>			
197	1	Twice annually, participate in an independent SSAE 16 Type II assessment from a VITA approved firm, covering all aspects of the Managed Environment.	Y	
198	2	Assessments or audits of the Managed Environment may be conducted by VITA, Customers, the Auditor of Public Accounts, the Managed Security Service Tower Supplier, or by federal agencies with oversight responsibilities. Such assessments may include risk assessments, forensic analysis or audits (e.g., AICPA's SOC 2, U.S. Internal Revenue Service 1075 audits, or risk assessments following NIST Special Pub 800-30 "Guide for Conducting Risk Assessments") of the Services being provided by Supplier and Service Tower Suppliers. These organizations reserve the right to define their own processes and methodologies to achieve their statutory goals. In such instances the Supplier shall:	Y	
199	2.1	Participate in assessments of the Security Program and Services provided by the Service Tower Suppliers.	Y	
200	2.2	Cooperate fully with and provide any assistance required by VITA and the assessment organization in support of these assessments or audits.	Y	
201	2.3	Provide access to any premises, equipment, personnel, documents, etc., as directed by VITA, the MSI or any other entity conducting such assessments or audits.	Y	
202	2.4	Recognize that VITA has sole discretion regarding acceptance or disputing any findings documented by such an assessment or	Y	
203	3	If the report concludes that the Security Program does not meet or exceed the VITA Rules, then the affected Service Tower Suppliers will develop and agree upon an Action Plan to promptly address and resolve any deficiencies, vulnerabilities, concerns and recommendations identified in such report, consistent with the affected Service Tower Supplier's obligations as	Y	
204	4	VITA will receive Deliverable Credits pursuant to <b>Exhibit 3.3 (Critical Deliverables)</b> should a Supplier fail to take remedial action in accordance with such Action Plan. Additionally, any system which has not been remediated in the defined period will be deemed to violate every Service Level associated with that system until it is remediated.	Y	

	A	B	C	D
205	5	Under no circumstances will Supplier attempt to persuade or control or otherwise influence the party conducting the Security Assessment.	Y	
206	6	Supplier acknowledges that VITA views the right to conduct assessments as a critical inducement to VITA's agreement to many of the terms of this Agreement, including the Term and termination rights provided for in the Agreement, and therefore Supplier agrees that it will cooperate in good faith to accomplish the objectives contemplated for the benefit of the	Y	
207		<b>4.8 Security Incident Management</b>		
208		<i>Security Incident Management is a specialized form of Incident Management, the primary purpose of which is the development and execution of well understood and predictable responses to damaging events, computer intrusions, security compromises and inadvertent data disclosure or destruction. As part of Security Incident Management, Supplier will provide the necessary resources to support Customers in resolving Security Incidents. The Supplier's responsibilities include:</i>		
209	1	Participate in the development of an Information Security Incident Management Plan (IS-IMP) in accordance with VITA Rules and in cooperation with the Customers.	Y	
210	2	Participate in the development of policies that govern the response to Security Incidents across the Managed Environment.	Y	
211	3	Participate in documenting and implementing the specific processes and tools for managing and responding to Security Incidents in support of the IS-IMP.	Y	
212	4	Utilize or integrate with the MSI provided tools for the tracking and recording of Security Incidents.	Y	
213	5	Security Incidents will be treated as Severity 1 Incidents.	Y	
214	6	Upon identification of a Security Incident, or potential Security Incident, follow the escalation notification processes in accordance with VITA Rules and the SMM.	Y	
215	7	Record timelines, actions, and events in accordance with SMM, VITA Rules, security requirements and the IS-IMP instructions.	Y	
216	8	Work to assist VITA, the MSI or designated Third-Party, with the investigation of Security Incidents and report findings to VITA, the MSI and designated parties.	Y	
217	9	Work with the MSI to create a Remediation Plan that is acceptable to VITA and Customers.	Y	
218	10	Execute the VITA approved Remediation Plan(s).	Y	
219	11	Participate with designated parties to conduct a forensic investigation to determine what Systems, data and information have been affected by the Security Incident.	Y	
220	12	Participate with designated parties to facilitate the identification of the initial point of entry into the Managed Environment, or other source of the Security Incident; including the tools and methods employed by the intruders, any data compromised, as well as a list of all other systems, Applications, or Third Parties potentially compromised.	Y	
221	13	Conduct investigation activities in conjunction with designated parties to maintain the data Integrity of any asset which may be needed for evidence.	Y	
222	14	Collect any data or Hardware deemed necessary by designated parties to assist with the Security Incident response, including logs, disk drives, files, servers, work-stations, and other items which may be of evidentiary value.	Y	
223	15	Maintain evidence integrity and strict chain of custody procedures for any items (physical or logical) relating to the Security Incident response investigation.	Y	
224	16	Assist VITA and designated parties in determining the impact and scope of suspected security breaches.	Y	
225	17	For all Security Incidents follow the Root Cause Analysis process identified in the SMM and work with designated parties for determining the underlying causes of a Security Incident.	Y	
226	18	Establish a Corrective Action Plan based on RCA findings that lead to actions that avoid or mitigate future Security Incidents.	Y	
227	19	Establish security leads and other roles as necessary that will have ownership and responsibility for working with designated parties and handling Security Incidents.	Y	
228	20	Coordinate with designated parties and participate in a Computer Security Incident Response Team (CSIRT) that is tasked to respond to Security Incidents in accordance with the SMM and VITA and Customer IT security requirements, processes and required response times.	Y	
229	21	As directed by the MSI, participate in routine Security Incident Management response exercises to validate the Security Incident response processes in accordance with the SMM.	Y	
230	22	Report results from the Security Incident Management response exercises and provide recommendations for improvements to the MSI.	Y	
231	23	Provide any logs or alert and event information required to respond to Security Incidents.	Y	
232	24	Do not serve any notice or otherwise publicize a Security Incident without the prior written consent of VITA.	Y	
233	25	Do not provide any information to outside sources (e.g., public, media, VITA or Supplier Personnel) of any Security Incidents without the prior written consent of VITA.	Y	
234	26	Cooperate with any law enforcement officials, regulatory officials, agencies or associations, where directed by the MSI or VITA and with the consent of VITA.	Y	
235	27	Provide reports of all Security Incident response details and activities in the Portal or other tools as defined in the SMM or requested by the MSI or VITA.	Y	

	A	B	C	D
236	28	Provide a summary of all Security Incidents related to the Services and Commonwealth Data to VITA, upon the request of VITA, for all Security Incidents since Commencement.	Y	
237		<b>4.9 Security Clearance Management</b>		
238		<i>The Supplier's responsibilities include:</i>		
239	1	Follow the documented clearance criteria in the SMM and mechanisms for accomplishing background checks as required by Customers and VITA Rules.	Y	
240	2	Conduct clearance reviews to include FBI background checks with fingerprints on all Supplier employees, contractors, subcontractors, and any other identified parties proposed to be assigned to perform Services prior to such assignment.  Note 1: Customers may elect to conduct such background checks themselves in lieu of Supplier, in which case Supplier will reimburse the Customers the costs incurred in performing such background checks.  Note 2: Supplier will not engage any employee, contractor or subcontractor in the performance of Services if the results of such person's background check and screening do not meet the established criteria. On a case-by-case basis, certain exceptions may be created by VITA.	Y	
241	2.1	Re-conduct background checks where clearance review criteria are required as specified in the SMM.	Y	
242	2.2	Individual clearance requirements must be completed and validated by VITA and the Customer prior to accessing any data owned by the Commonwealth.	Y	
243	2.3	Review and update the clearance review criteria required by VITA and the Customers on an annual basis.	Y	
244	3	Remove from the VITA account any Supplier employee, contractor or subcontractor whose background check results do not meet the criteria acceptable to VITA and the requirements of the Customers.	Y	
245	4	Ensure that all persons having been cleared are documented with the identified clearance (e.g., background checks, training) in the Security Clearance System.	Y	
246	5	Follow reporting procedures, in the SMM, which support immediate notifications to Customers of personnel who are added to or departed from the contract.	Y	
247	6	Ensure upon personnel separation all issued badging, Devices, access materials, etc. are returned to the Supplier prior to leaving Supplier's control. All Customer issued badging, devices, access materials, etc. must be returned to the Customer or VITA designated party within 7 calendar days.	Y	
248		<b>4.10 Security Clearance System</b>		
249		<i>The Security Clearance System is a Service Management System. The Supplier's responsibilities include:</i>		
250	1	Utilize the Security Clearance System as provided by the MSI.	Y	
251	2	Limit access to the Security Clearance System to the agreed levels established in the SMM for the type of Supplier Users who require access to the systems.	Y	
252	3	Participate in MSI-required training in using the Security Clearance System.	Y	
253	4	Ensure all data fields for which the Supplier is responsible are accurate and complete.	Y	
254		<b>4.11 Risk Management</b>		
255		<i>In collaboration with, and coordinated through the MSI, Supplier is charged with providing Risk Management related to the IT environment and Services within the context of the ITISP overall business risks. The goal of Risk Management is to quantify the impact to the business that a loss of Service or asset would have (the Impact), to determine the likelihood of a threat or exploitation of a vulnerability to actually occur, and then to manage activity against the identified risk. The Supplier's</i>		
256	1	Utilize the framework for risk management provided by the MSI for the Services, including:	Y	
257	1.1	Document, implement and maintain sections of the SMM to include the VITA risk policies, processes, tools and standards pertaining to Supplier in accordance with the NIST Risk Management Framework.	Y	
258	1.2	Coordinate initial Supplier implementation and ensure continual maintenance of standard tools and processes for risk management as determined by the Risk Management Framework.	Y	
259	1.3	Support the appropriate governance forums with specific risk content as requested by the MSI.	Y	
260	2	Utilize risk indicators across the Services to monitor risk and assist the detection of emerging trends and control failures (reference Event Management).	Y	
261	3	Integrate the governance, risk and compliance tool(s) with the CMDDB, with two-way data exchange.	Y	
262	4	Integrate activities with Event Management to detect risks and emerging trends.	Y	
263	5	Assist the MSI in creating a Plan of Actions and Milestones (POAM) detailing the plan to remediate or mitigate risks within the timeframe established by VITA or the Customer and implement risk escalation and reporting across the Services.	Y	
264	6	Support risk escalation and reporting.	Y	
265	7	Address known control weaknesses with controls operated within the existing Services as notified to the Supplier.	Y	
266	8	Provide proposals to address new control requirements and propose options with costs for implementing such controls and mitigating the risks to the Customers.	Y	

	A	B	C	D
267	9	Utilize the solution that provides access for Customers and the Service Tower Suppliers to common risk and controls information, including reports, risk logs, Action Plans, key controls and risk indicator data.	Y	
268	10	Participate in monthly, or as outlined in the SMM, reviews with the MSI regarding the effectiveness of controls to ensure compliance with regulations and Customers policies. Reviews will include:	Y	
269	10.1	Progress in addressing risks that need to be mitigated in the Suppliers' Services.	Y	
270	10.2	Emerging trends and risks.	Y	
271	10.3	The effectiveness of key controls.	Y	
272	10.4	Progress in addressing known control deficiencies – arising from the Supplier's own assurance activities, audits, any SSAE 16 reviews and any Customer or Supplier assurance activity.	Y	
273	11	Participate in monthly, or as outlined in the SMM, forum with all of the other Service Tower Suppliers, the MSI, VITA designated entities and ITISP Governance and provide:	Y	
274	11.1	Progress in addressing risks that need to be mitigated in the Suppliers' Services.	Y	
275	11.2	Emerging trends and risks.	Y	
276	11.3	The effectiveness of key controls.	Y	
277	11.4	Progress in addressing known control deficiencies – arising from the Supplier's own assurance activities, audits, any SSAE 16 reviews and any Customer or Supplier assurance activity.	Y	
278	<b>4.12 Risk Monitoring, Identification, and Reporting</b>			
279	<i>The Supplier's responsibilities include:</i>			
280	1	Participate in regular, formal risk assessments, in accordance with VITA Rules and SMM, Customers and the MSI, and document the results.	Y	
281	2	Report risks using a standard operational risk register, which will be maintained by the MSI for all the ITISP Services and available for Users (Users may be limited, i.e., not all Users) as defined in the SMM.	Y	
282	3	Provide on-going monitoring of the operations for change and emerging risks and trends.	Y	
283	4	Report and escalate these trends, changes and emerging risks through the MSI to VITA and ITISP Governance.	Y	
284	5	Monitor Incidents and assess those that could have, or did, result in loss to Customers to ensure risks of a repeat are assessed and mitigated.	Y	
285	6	Identify and report risks, including the Service impact assessment, arising from the activities in the delivery of the end-to-end	Y	
286	7	Support the activities of Customer's staff, auditors or regulators in conducting assurance activities on the design and effectiveness of key controls across the end-to-end Services.	Y	
287	8	Report on the activities to address any control weaknesses identified in the above assurance activities.	Y	
288	<b>4.13 Risk Prevention and Mitigation</b>			
289	<i>The Supplier's responsibilities include:</i>			
290	1	Take appropriate proactive actions to prevent or mitigate new or emerging risks for the Services.	Y	
291	2	Manage all risks assigned by VITA, including identifying and implementing treatments to mitigate the risks for the Services.	Y	
292	3	Participate in regular risk assessments, in accordance with the SMM, and in compliance with VITA Rules.	Y	
293	4	Support the preparation of proposals for approval by VITA that meet Customers' control objectives and requirements for changes to existing key controls or new key controls to prevent or mitigate risks. At a minimum, the risk treatment plan will	Y	
294	4.1	Goals and objectives.	Y	
295	4.2	Scope.	Y	
296	4.3	Audience.	Y	
297	4.4	Asset and attribute details.	Y	
298	4.5	Risks.	Y	
299	4.6	Existing controls.	Y	
300	4.7	Controls to be implemented.	Y	
301	4.8	Actions to be taken.	Y	
302	4.9	Roles and responsibilities.	Y	
303	5	Implement key controls, and changes to existing controls, to address risks.	Y	
304	6	Assist the MSI in conducting and reporting on Risk Assessments that will, at a minimum, include:	Y	
305	6.1	Assets:	Y	
306	6.1.1	Asset name.	Y	
307	6.1.2	Asset category.	Y	
308	6.1.3	Asset owner.	Y	
309	6.2	Risk assessment:	Y	
310	6.2.1	Risk analysis (threats and vulnerabilities).	Y	
311	6.2.2	Business impact.	Y	
312	6.2.3	Likelihood.	Y	
313	6.2.4	Risk evaluation.	Y	

	A	B	C	D
314	6.3	Risk treatment (controls):	Y	
315	6.3.1	Risk appetite.	Y	
316	6.3.2	Risk mitigation.	Y	
317	6.3.3	Controls.	Y	
318	6.4	Risk residual.	Y	

Ref #	Requirement	Comply (Y/N)	Supplier Response
	<b>5.0 MCS Program Management</b>		
	<b>5.1 General MCS Program Management Requirements</b>		
	<i>The supplier's responsibilities include:</i>		
1	Provide the strategic management, processes and tools necessary for the MCS provider's team to manage the overall program of services as the Managed Cloud Services supplier.	Y	
2	Operate, manage, and support VITA owned licenses, components, and services in both Commercial and Government Cloud environments.	Y	
3	Accountable for the processes and tools necessary for the MCS provider's team to promote rapid delivery of compliant solutions with frictionless service integration among Service Tower Suppliers.	Y	
4	Provide account management team for single point of contact to VITA leadership	Y	
5		Y	
6	Provide transition-in leadership team and accountability when onboarding with VITA as a new supplier. Achieve the successful completion of the integration points listed in <b>Exhibit 2.4.2 (Implementation Integration Points)</b> . Refer to <b>Exhibit 2.4 (Implementation Plan)</b> for detailed implementation requirements.	Y	
7	Process any Request For Solution (RFS) per SMM 4.1.5.8 Request for Solution & Estimate that the incumbent supplier has not fulfilled. A list of current and planned projects are listed in <b>Exhibit 2.6 (Current-Planned Projects)</b> .	Y	
8	Per <b>SMM 4.1.4.5 Knowledge Management</b> , provide training to stakeholders in the VITA MSI platform, orienting them to the MCS services and how to operationalize them. Stakeholders include Agencies, VITA, and Service Tower Suppliers.	Y	
9	Provide efficient industry standard models for cloud consumption by providing shared resources, automation, and	Y	
10	Guide agencies and provide ongoing support in developing cost optimized architecture.	Y	
11	Identify opportunities to lower the platform's barrier to adoption through activities such as:	Y	
11.1	Infrastructure and Platform as Code.	Y	
11.2	Industry standard CI/CD tools and workflows.	Y	
11.3	Infrastructure provisioning to enable platform scale, and extend the platform's capabilities.	Y	
11.4	Automate routine tasks and processes. Additionally, introduce efficiencies to approved automated tasks.	Y	
11.5	Enable a native cloud-first approach to security controls & toolsets.	Y	
11.6	Enable more native cloud technologies vs. on-prem to minimize on-prem dependencies.	Y	
11.7	Provide reporting on established cloud resources that do not align to Commonwealth Security requirements.	Y	
11.8	Prohibit the creation of new cloud resources that do not align to Commonwealth Security requirements.	Y	

Ref #	Requirement	Comply (Y/N)	Supplier Response
	<b>6.0 MCS Delivery Operations</b>		
	<i>The Operations Group will provide operational support, implementation support, maintenance, and disaster recovery services. This team must meet all service level agreements on a monthly basis and achieve VITA's acceptance on all periodic critical deliverables.</i>		
	<b>6.1 MCS Delivery Operations requirements</b>		
	<i>The Supplier's responsibilities include:</i>		
1	As per <u>SMM 4.1.3.2 Service Catalog Management</u> , supplier will Catalog, Provision and Optimize services in the enterprise service catalog after completing <u>SMM 4.1.2.4 Service Portfolio Management</u> and <u>SMM 4.1.3 Service Design</u> , along with any SMMs referenced in those documents. Support the MSI in maintaining entries in VITA's service catalog with frictionless workflows for rapid approvals and provisioning CSP services.	Y	
2	Integrate with the MSI's <u>SMM 4.1.6 Continual Improvement</u> and MSI Cloud Broker Technology Integration process (CBTI).	Y	
3	Manage rapid provisioning timeframes by assembling standard packaged services with approved configurations, with simple account registration, activation of in-scope features, and policy-compliant	Y	
4	Create, configure, and deploy solutions in response to requests for service from VITA and its agency customers., as per <u>SMM 4.1.3.1 Solution Design Management</u> , <u>SMM 4.1.5.5 Service Request Management</u> , <u>SMM 4.1.4.3 Release and Deployment Management</u> , <u>SMM 4.1.4.1 Change Management</u> , among others.	Y	
5	Provision cloud environments and confirm all systems are proactively managed to meet defined service levels.	Y	
6	Coordinate and collaborate with the MSI's CBTI to enable agency stakeholder consumption management activities	Y	
	<b>6.2. Operations, Maintenance, and Monitoring</b>		
	<i>The Supplier's responsibilities include:</i>		
1	Control all In-Scope computer platforms and associated Infrastructure throughout the organization.	Y	
2	Provide service event management teams 24/7/365 reviewing alerts and managing incidents, requests, and other processes as listed in <b>Tab 2.0 (Cross Functional Services)</b> . ( <u>SMM 4.1.5.3 Monitoring and Event Management</u> )	Y	
3	Notify the appropriate stakeholders in accordance with the <u>SMM 4.1.5.2 Incident Management</u> , <u>SMM 4.1.5.3 Event Management</u> , <u>SMM 4.1.5.5 Service Request Management</u> , among other SMMs, in the event that Applications do not execute properly.	Y	
4	Analyze performance metrics and reports, and respond proactively to potential issues, per <u>SMM 4.1.6.3 Service Measurement</u> , among others..	Y	
5	Assume the responsibility for and perform all operations Functions:	Y	
5.1	Monitor all processing for failures, incidents, problems, and other events that impair in-production services.	Y	
5.2	Monitor all phases of Systems performance using appropriate real-time and historical data performance.	Y	
5.3	Provide performance monitoring and tuning of Supported Equipment and Systems.	Y	
5.4	Monitor the performance of online interactive traffic and take appropriate action to Resolve online-system-related Incidents, including escalating (as appropriate) the Incident in accordance with the <u>SMM 4.1.5.2 Incident Management</u> .	Y	
5.5	Support, monitor, and log the transmission of files within the scope of the MCS responsibilities for the CSP environments as designated by Customers and consistent with VITA Rules.	Y	
5.6	Provide end-to-end visibility to MSI and VITA-approved Users or VITA Customers to view performance statistics (real-time and historical) on all Infrastructure Services.	Y	
5.7	Supplier will provide their own Microsoft Unified Support agreement, and similar arrangements with other components of their solutions. Supplier will not be able to utilize the VITA support agreements.	Y	
6.0 MCS Delivery Operations	General		

6	Perform periodic and emergency Systems maintenance in accordance with <u>SMM 4.1.4.1 Change Management</u> to minimize the Impact to VITA and VITA Customers.	Y	
7	Perform computer shutdowns and restarts, as required, and execute customary utility Functions.	Y	
8	Maintain, administer, and provide necessary automated tools and processes for Systems management to the extent available in the tool suite jointly agreed by the Supplier and VITA.	Y	
9	Run or terminate utilities and processes depending upon the Impact to Users/Systems and only with the <u>appropriate VITA or Customer Approvals</u> .	Y	
10	Per <u>SMM 4.1.4.5 Knowledge Management</u> , collect knowledge of processing requirements, remote operational Support, and any other Support for transitional Services in Support of Data Center and/or cloud to cloud migrations and business acquisitions and divestitures. Supplier documents the actions and key services via Knowledge Base Articles within Keystone Edge portal service management system. This is to aid in <u>proper assignments and routing of tickets to the supplier based on service provisioning and execution</u> .	Y	
11	Perform preventive maintenance, including:	Y	
11.1	Perform all maintenance according to the manufacturer's Specifications.	Y	
11.2	Provide documentation to the MSI to establish standard changes for the MCS supplier scope, and workflows in Change Management System that will be used to plan, execute, and verify that preventive maintenance has been completed.	Y	
12	Perform daily backups of Configurations in order to recover/restore Services in accordance Customer requirements.	Y	
13	Perform Storage management for varying types of cloud resources.	Y	
14	Perform Performance, Health, Monitoring, Reporting (including dashboards available to any stakeholder group)	Y	
15	Perform Hardened image management.	Y	
16	Perform Automated cloud lifecycle management including but not limited to data management or account access management in alignment with VITA Rules and Customer requirements.	Y	
17	Use framework automation, infrastructure automation, and deploy integration modules as appropriate and <u>approved by VITA and Customer</u> .	Y	
18	Perform Continual improvement, per <u>SMM 4.1.6 Continual Improvement</u> , through applied intelligence, analytics, and automation to drive efficiencies and flexibility.	Y	
19	Perform System performance tuning necessary to achieve performance metrics including service level agreements and other requirements, per <u>SMM 4.1.3.3 Service Level Management</u> .	Y	
20	Configuring, adding, and deleting file systems.	Y	
21	Answering technical queries and assisting Users.	Y	
22	Host its own CMDB in its internal tools, and integrate it to the MSI Configuration Management Database (Enterprise CMDB) per <u>SMM 4.1.4.4 Service Asset &amp; Configuration Management</u> . The data and configuration of the Supplier's CMDB is VITA property, but the tool itself is the Supplier's property.	Y	
23	Performing routine audit of Systems and Software (configuration, licenses, compliance with VITA rules, etc.).	Y	
24	Work and coordinate with other MCSs, MSI's CBTI, and VITA to address interconnectivity and functionality between CSPs in support of agency solutions and requirements.	Y	
<b>6.3 Patch Management</b>			
<i>The Supplier's responsibilities include:</i>			
1	Patch Systems in compliance with VITA Rules. Create for review and approval any MCS supplier-specific written process in SMM 8.x section.	Y	
2	Ensure that all Devices and Enterprise Supported Software in the environment (Physical and Virtual) are Patched and maintained (e.g., Operating System Security Patches, performance Patches, firmware, service packs, Versions) in accordance with VITA Rules and the SMM.	Y	
3	Provide Reports on the status of Patching every 30 days and upon request in accordance with the SMM.	Y	

4	Patch enterprise Equipment, Systems, Software, and other Devices that are part of Infrastructure Services. Use the approved central Software deployment tool and deploy Patches to Servers and clients per Customer's policies as defined in the SMM.	Y	
5	The results of Patch management piloting process to the MSI, Impacted Customers and VITA within 24 hours of Patching activities.	Y	
6	In the event that the Patch process disrupts Customer operations the Supplier shall roll back the changes made in accordance with the SMM.	Y	
7	Apply Patches to Devices & Applications within the timeframe guidelines in accordance with Customer's Security policies and the SMM.	Y	
8	Communicate with and/or alert the Customer IT Security team when Patches are not Installed within the designated timeframe. Provide a plan to remediate.	Y	
9	Integrate and have the ability to export Patch data associated will all Customer Devices.	Y	
10	All non-security related IT solutions and supporting software shall have patches applied to systems in accordance with VITA Rules. (e.g., operating system security patches, performance patches, firmware, service packs).	Y	
<b>6.4 Technical Support</b>			
<i>The Supplier's responsibilities include providing subject matter expertise and technical support for the requirements that follow, to include standards, guidelines and usage patterns of provided services.</i>			
1	Provide all technical Support for provided MCS solutions and applications.	Y	
2	Create for review and approval any MCS supplier-specific written process in SMM 8.x section as it relates to Supplier provided services for operations of all provided services, including but not limited to:	Y	
2.1	Server administration	Y	
2.2	Storage management	Y	
2.3	System administration	Y	
2.4	Virtual Server Support	Y	
2.5	Install/Move/Add/Change (IMAC)	Y	
2.6	Capacity planning	Y	
2.7	Performance tuning	Y	
2.8	Problem Resolution and Root Cause Analysis	Y	
2.9	Configuration Management	Y	
2.10	Service Availability	Y	
2	Install and maintain all System Software products in accordance with <u>SMM 4.1.4.1 Change Management</u> , <u>SMM 4.1.4.2 Change Evaluation</u> , and <u>SMM 4.1.4.3 Release and Deployment</u> .	Y	
3	Provide technical advice and Support to the MSI, VITA, VITA Customer and other Supplier Application Development and Maintenance staffs as required.	Y	
4	Provide appropriate response and support to Incidents and continued troubleshooting Support through Resolution, as required, to meet the Service Levels in accordance with the <u>SMM 4.1.5.2 Incident Management</u> .	Y	
5	Participate in Change Management process and groups implementing Changes in accordance with <u>SMM 4.1.4.1 Change Management</u> , <u>SMM 4.1.4.2 Change Evaluation</u> , <u>SMM 4.1.4.3 Release and Deployment</u> , and <u>SMM 4.1.4.4 Service Asset and Configuration Management</u> , among others.	Y	
6	Monitor Customers' data Storage media and processor utilization and requirements per <u>SMM 4.1.5.3 Monitoring and Event Management</u> .	Y	
7	Adhere to Documentation standards in accordance with the <u>SMM 1.2 Documentation Management</u> , among others, and VITA Rules.	Y	
8	Develop, where appropriate, and Install Productivity Suites, as well as performing all required operational modifications for the efficient and proper delivery of the Services.	Y	
9	Develop and maintain technical and functional Specifications and requirements for all environments and related interfaces per <u>SMM 4.1.4.4 Service Asset and Configuration Management</u> .	Y	

10	Provide product research, Project Support, and advice on Equipment and Application tuning and efficiency improvements.	Y	
11	Install, tailor, maintain and provide ongoing Support for System Software products in accordance with the SMM.	Y	
12	Install Software and configure Services according to the Applications' Specifications, the SMMs, and VITA Rules.	Y	
13	Coordinate Software Upgrades and Updates with MSI, VITA and VITA Customers as per <u>SMM 4.1.4.1 Change Management</u> .	Y	
14	Report generally available performance data and resource utilization statistics related to System Software release-level Upgrades.	Y	
15	Provide Support regarding VITA and/or VITA Customer Requests (e.g., product research, Project Support, and advice on Equipment tuning and efficiency improvements, as well as on Applications tuning and efficiency improvements.) as per <u>SMM 4.1.5.5 Service Request Management and Fulfillment</u> .	Y	
<b>6.5 Capacity Management</b>			
<i>The Supplier's responsibilities include:</i>			
1	Perform activities required for ongoing monitoring and optimizing performance to reduce costs or improve Service Levels.	Y	
2	Provide Systems performance reviews and advice per <u>SMM 4.1.3.6 Capacity Management</u> .	Y	
3	Conduct and report on System performance testing when required.	Y	
4	As per <u>SMM 4.1.4.1 Change Management</u> , perform Infrastructure, Software, and Service upgrades as required to provide effective capacity and to meet VITA, VITA Customer, and Software architectural requirements. Using VITA defined Change Control process.	Y	
5	Coordinate with business partners, Third Party Vendors, other vendors as appropriate, and VITA and VITA Customers on Projects to Install and Upgrade Infrastructure Devices.	Y	
<b>6.6 User Support</b>			
<i>The Supplier's responsibilities include:</i>			
1	Provide Support, advice, and assistance to VITA Users in accordance with <u>SMM 4.1.5.1 Service Desk</u> , among	Y	
2	Perform and provide analysis to provide optimal use of production resources.	Y	
3	Perform changes for programmers and Users as requested by an authorized VITA or VITA Customer representative in accordance with the <u>SMM 4.1.5.5 Service Request Management</u> , <u>SMM 4.1.5.8 Request for Solution and Estimate</u> , among others.	Y	
4	Provide technical Support and administration for various products and Application rollouts to VITA and VITA Customers in accordance with the <u>SMM 4.1.1.2 Project Portfolio Management</u> , among others.	Y	
<b>6.7 Personnel/Clearance Management</b>			
<i>The Supplier's responsibilities include:</i>			
1	Grant VITA approval rights for key personnel interfacing with VITA and VITA Customers and the right to review qualifications for any-and-all staff servicing VITA and- VITA Customers.	Y	
2	Grant VITA Customers rights to review qualifications for any-and-all staff servicing that Customer per <u>SMM 8.1.3 Background Checks and Security Clearance Process</u> .	Y	
3	Provide controls and ensure that advanced Security operations Functions and escalation roles are performed by senior staff cleared to conduct those Functions and roles.	Y	
4	Provide controls in support of <u>SMM 8.1.3 Background Checks and Security Clearance Process</u> , <u>SMM 8.2.3 Security Clearance Tracking</u> , among others, or as directed by VITA and/or VITA Customers (i.e. IRS training requirements), and ensure that personnel complete all mandatory training in accordance with the SMM.	Y	
5	Personnel shall immediately disclose any changes that may Impact their background check results in accordance with VITA Rules.	Y	

VA-240920-NTT: Managed Public Cloud Services

Ref #	Requirement	Comply (Y/N)	Supplier Response
	<b>7.0 MCS Solution Management</b>		
	<b>7.1 MCS Business Solutions Management General Requirements</b>		
	<i>The suppliers responsibilities include:</i>		
1	Staff and deploy a dedicated Business Solutions Management team.  Note: BSM team members are assigned to agency application and business organizations charged with engagement with the agency customers, with a goal to remove uncertainty and instill confidence in the MCS services. BSM Team provides agency-assigned solution engineering and manager resources to handle MCS related RFS solutioning, complaints, disputes, and issues.	Y	
2	Provide baseline staffing to solution and fulfil RFS, customer backlogs, and demand management for the delivery of professional services.	Y	
3	Describe the staffing model and relevant pricing for how the supplier intends to support the Request for Solution process. The monthly volume of RFS solution requests will require a base capacity on the Solutions Management team. As volume increases, describe how capacity is added to the Solutions Management team's throughput to maintain SLA compliance, avoiding delays or quality-of-solution issues.	Y	
4	Ability to propose, justify, and staff substantial software engineering efforts for agencies able to fund them, with Supplier staff or via subcontractor. Provide application development services that emphasize application-focused R's. Rehost, revise, rearchitect, rebuild and replace are generally considered the five R's of cloud transformation. Rehost (lift and shift) and some portion of revise are considered infrastructure-led activities, while the remaining R's (rearchitect, rebuild and replace) are the focus of application-led transformation services.	Y	
5	Describe the ability to provide 2 week and other duration types of Agile Sprints. These descriptions should include the resources in each type of sprint and the capacity of the sprints.	Y	
6	Upskill CoV personnel. Provide training, CSP-centric certifications, and coaching for agency personnel that encourages awareness of cloud services value, agency-level teams self-service, and creative solutioning.	Y	
7	Design and execute a communications plan and knowledge management practices per the <u>SMM 11.1 Communication Management</u> , <u>SMM 4.1.4.5 Knowledge Management</u> , among others, and approved by VITA via the MSI Governance processes, to include varied information methods that effectively inform customers of the services and value they may create via implementation of the services.	Y	
8	Offer webinars/training on new CSP or MCS offerings.	Y	
9	Establish then enable agencies to contribute to a COV Cloud body of knowledge by sharing information about their deployments and expertise to other agencies.	Y	
10	Participate in VITA's electronic social communities (i.e. blogs, forums, knowledge base articles, webinar, etc.) where customers can get guidance, ask questions, leave feedback, etc. Additionally archive any hosted webinars for future playback by Customers to support continued development of the Body of Knowledge. Additional information is found in <b>Exhibit 3.5 (Customer Satisfaction)</b> .	Y	

11	Deliver architecture and engineering consulting for designing, development, and deploying solution development, including services capable of the following scope:	Y	
11.1	Perform Cloud strategy assessment, in-scope to the Supplier, including situations involving "Bring your own	Y	
11.2	Perform Cloud solution architecture design and documentation.	Y	
11.3	SaaS advisory services (help client know what can move to SaaS).	Y	
12	Perform Migration planning:	Y	
12.1	Supplier will deliver a detailed planning model to be used by the Agencies to estimate the number of hours per resource type needed to migrate an application, tenant, resource, etc.	Y	
12.2	Defined agency resource roles	Y	
12.3	Hours needed by resource role taking into consideration complexity of application and the Services that need to be migrated.	Y	
12.4	Provide a mechanism for customers to calculate or estimate costs associated with the migration.	Y	
12.5	Provide a mechanism for customers to calculate or estimate future costs associated with post migration run costs/rates in the Cloud (such as 1/5/10 year costs).	Y	
13	Perform Migration implementation services as requested (workload discovery, assessment and movement).	Y	
14	Support the enablement and deployment of DevSecOps principles and tools.	Y	
15	Perform Ongoing, day-to-day advice and cloud transformation assistance.	Y	
16	Provide services to customers for business solutions management or consulting (assessment, strategy, migration planning and implementation) services.	Y	
17	Solution, support, and manage "bring your own" CSP tenants that Customers own and bring into compliance with VITA Rules.	Y	
<b>7.2 Enhanced (Optional) Services</b>			
<i>As part of fulfilling an RFS, the supplier may be asked to perform the following additional services:</i>			
<i>Note: Suppliers are encouraged to list other Enhanced Services which they are capable of providing in the rows</i>			
1	Provide other optional services to customers who wish to purchase them (system integration, application development, application management, management of on-cloud infrastructure, refactoring, reimplementation, or other IT outsourcing services) unrelated to their core cloud-managed services.	Y	

VA-240920-NTT: Managed Public Cloud Services

Ref #	Requirement	Comply (Y/N)	Supplier Response
	<b>8.0 Cloud Service Provider Specific Requirements</b>		
	<i>Offerors shall only complete the below section for the CSP for which they are submitting their response. The other two (2) CSP sections shall be left intentionally blank.</i>		
	<b>8.1 Microsoft Azure</b>		
	<i>The Supplier's responsibilities shall include:</i>		
1	An active, current, and maintained Azure Expert MSP with the Modernization of Web Applications to Microsoft Azure advanced specialization. <a href="https://azure.microsoft.com/en-">https://azure.microsoft.com/en-</a>	Y	
2	The ability to support existing Microsoft CSP licensing and Microsoft EA licensing.	Y	
3	Demonstrated ability to migrate Microsoft CSP licensing to Microsoft EA licensing. The supplier shall provide evidence of their abilities to do so in <b>Administrative Appendix B (Supplier</b>	Y	
4	Present proof of Azure Certification(s) for any personnel providing services to VITA.	Y	
5	Make Azure Services data available to customers via the MSI's CBTI platform. Enable access to the VITA-approved portfolio of Azure Services. This data sets includes technical services and options, any available reporting tools, all Azure user portal services and options including the billing data, and all Azure	Y	
6	Onboard each Agency, then provide the capability for Agencies to use the CBTI toolset to manage its own Azure consumption, with the autonomy to scale up and down and add approved services as needed.	Y	
7	Possess and maintain the resources to work with multiple entities at the same time.  <i>Note: There are more than 60 Executive Branch agencies in-</i>	Y	
8	Maintain expertise, resources and capabilities throughout the life of the contract to perform the following:		
8.1	Perform consulting, assessment, design, integration, installation, and managed Services and Solutions in the Request for Service (RFS) process	Y	
8.2	Provide professional, technical support and engineering services to support the Commonwealth Agencies business needs related to the Azure.	Y	
8.3	Provide maintenance support of the services and solutions.	Y	
8.4	Provide agency-specific and overall contract performance reporting, as required.	Y	
8.0	Ability to Provide Red support Infrastructure as a Service (IaaS)	Y	

8.0 Cloud Service Provider Red

Sensitivity Label: General

10	Ability to provide and support Software as a Service (SaaS)	Y	
11	Ability to provide and support Platform as a Service (PaaS)	Y	
12	Ability to provide and support Database as a Service (DbaaS)	Y	
13	Describe other offerings that you can provide and support.	Y	
14	Provide governance and management that aligns with Microsoft's Cloud Adoption framework.	Y	
<b>8.2 Google Cloud Platform (GCP)</b>			
	<i>The Supplier's responsibilities shall include:</i>		NTT DATA is not providing GCP services
1	An active, current, and maintained Google Cloud MSP Partner with the Application Development specialization		
2	Present proof of GCP Certification(s) for any personnel providing services to VITA.		
3	Make GCP services available to customers. Enable access to the VITA-approved portfolio of GCP Services. This includes technical services and options, any available reporting tools, all GCP user portal services and options, any available reporting tools, all GCP user portal services including the billing portal, and all GCP technical support services.		
4	Onboard each Agency, then provide the capability for Agencies to use the CBTI toolset to manage its own GCP consumption, with the autonomy to scale up and down and add approved services as needed.		
5	Possess and maintain the resources to work with multiple entities at the same time.		
6	Note: There are more than 60 Executive Branch agencies in- Maintain expertise, resources and capabilities throughout the life of the contract to perform the following:		
6.1	Perform consulting, assessment, design, integration, installation, and managed Services and Solutions in the Request for Service (RFS) process		
6.2	Provide professional, technical support and engineering services to support the Commonwealth Agencies business needs related to the GCP.		
6.3	Provide maintenance support of the services and solutions.		
6.4	Provide agency-specific and overall contract performance reporting, as required.		
7	Log all administrative access and integrate to SIEM as required by VITA. This requires that the cloud provider can sync AA / ZZ / etc. or other privileged accounts. GCP would need such accounts to have an SMTP address configured in order to sync		
8	Manage user account information and Lifecycle to support Google integration while complying with VITA Rules		

9	Ability to provide and support Infrastructure as a Service (IaaS)		
10	Ability to provide and support Software as a Service (SaaS)		
11	Ability to provide and support Platform as a Service (PaaS)		
12	Ability to provide and support Database as a Service (DBaaS)		
13	Describe other offerings that you can provide and support.		
<b>8.3 Oracle Cloud Infrastructure (OCI)</b>			
	<i>The Supplier's responsibilities shall include:</i>		NTT DATA is not providing OCI services
1	An active, current, and maintained Oracle Cloud Solutions Provider certification(s). <a href="https://www.oracle.com/partnernetwork/expertise/cloud-solutions-provider/">https://www.oracle.com/partnernetwork/expertise/cloud-solutions-provider/</a>		
2	Present proof of OCI Certification(s) for any personnel providing services to VITA.		
3	Make OCI services available to customers. Enable access to the VITA-approved portfolio of OCI Services. This includes technical services and options, any available reporting tools, all OCI user portal services and options, and all OCI technical support		
4	Onboard each Agency, then provide the capability for Agencies to use the CBTI toolset to manage its own OCI consumption, with the autonomy to scale up and down and add approved services as needed.		
5	Possess and maintain the resources to work with multiple entities at the same time.  <i>Note: There are more than 60 Executive Branch agencies in-</i>		
6	Maintain expertise, resources and capabilities throughout the life of the contract to perform the following:		
6.1	Perform consulting, assessment, design, integration, installation, and managed Services and Solutions in the Request for Service (RFS) process		
6.2	Provide professional, technical support and engineering services to support the Commonwealth Agencies business needs related to the OCI.		
6.3	Provide maintenance support of the services and solutions.		
6.4	Provide agency-specific and overall contract performance reporting, as required.		
7	Ability to provide and support Infrastructure as a Service (IaaS)		
8	Ability to provide and support Software as a Service (SaaS)		
9	Ability to provide and support Platform as a Service (PaaS)		
10	Ability to provide and support Database as a Service (DBaaS)		
11	Describe other offerings that you can provide and support.		

## VA-240920-NTT: Managed Public Cloud Services

Ref #	Requirement	Comply (Y/N)	Supplier Response
	<b>9.0 Assumed Services</b>		
	<i>The following list of services and activities should be used by Suppliers as a view of the current services being provided. These services may need to be continued until the transition of services is completed. CSP specific assumed services, may need to be continued even after the transition has been completed.</i>		
	<b>9.1 Common Platform Services</b>		
1	Assume responsibility for and perform all console functions and operations.	Y	
2	Install, configure, monitor and support tools for the collection of detailed information required for SLAs, reports and invoicing.	Y	
3	Ensure the implementation of system management and monitoring for servers, services, functions and other billable service components in the virtual public cloud in accordance with the <u>SMM 4.1.5.3 Event Management, SMM 4.1.3.4 Availability Management, SMM 4.1.3.5 Service Continuity Management, among others.</u>	Y	
4	Manage and monitor server performance and utilization of the various server resources necessary to provide optimum services performance (e.g., CPU, file system level Storage, memory, Server Network interface throughput).	Y	
6	Monitor the performance of online interactive traffic and, in accordance with the SMM, take appropriate actions to resolve online System related Incidents and/or Problems, including escalating (as appropriate) the Incident and/or Problem to the proper Support group.	Y	
7	Operate terminal and jump servers for Customers.	Y	
8	Provide capability for VITA and VITA Customers to utilize the enterprise management and monitoring tools and/or deploy Customer specific monitoring and management agents (e.g., SCOM).	Y	
9	Build Application packages, based on Customer requirements, for deployment.	Y	
10	Deploy the packages based on release schedules in accordance with the SMM.	Y	
11	Provide ongoing coordination and support for Customer Application groups.	Y	
12	Perform load balancing in coordination with the Customers and Authorized Third Party Vendors.	Y	
13	Purge records and file old User accounts upon VITA-approved User's request and in accordance with VITA and VITA Customer records retention policies.	Y	
14	Restore archived or deleted files upon VITA-approved User's request.	Y	
15	Perform regular monitoring of utilization needs and efficiencies, and report regularly on tuning initiatives.	Y	
16	Perform or obtain proactive failure trend analysis.	Y	
17	Produce trend reports to highlight production Incidents and Problems and establish predetermined action and escalation procedures when batch window Incidents and Problems are encountered.	Y	
18	Notify the MSI and affected VITA Customers, in accordance with the notification procedures, in the Event that Applications do not execute properly.	Y	
19	Perform periodic and Emergency Systems maintenance in accordance with Procedures established in the SMM to minimize the impact to Customers' businesses.	Y	
20	Perform computer shutdowns and restarts, as required, and execute customary utility functions.	Y	
21	Maintain shutdown and restart order and dependency documentation for all Systems and their Services/Processes for a Site.	Y	
22	Gather and maintain order and dependency information, by VITA and VITA Customer business priorities.	Y	
23	Maintain, administer, and provide necessary automated tools and processes for systems management to the extent available in the VITA-approved tool suite or as required to be delivered by Supplier elsewhere in the Agreement.	Y	
24	Maintain tables, calendars, parameters, and definitions for tools used to automate manual Procedures or to automate and improve the quality of the operations.	Y	

25	Provide remote monitoring and management for all software, functions, and other billable service components.	Y	
26	Maintain and update the operational documentation for all operations procedures and Services, including maintaining accurate information about all CIs in the CMS / CMDB.	Y	
27	Provide guidance for active prevention of Service performance events (e.g. CPU, file system level Storage, memory, Server, Network interface throughput.)	Y	
28	Provide threshold levels at a Server or Application level, per VITA and VITA Customer guidelines.	Y	
29	Analyze performance metrics and respond proactively to potential Problem areas.	Y	
30	Suspend, disable, or remove Users in accordance with procedures and relevant notifications developed and documented with VITA and VITA Customers' input and Approval.	Y	
31	Provide routine administrative Services, such as print queue setup, print table setup rights, as well as administration and password administration as requested by VITA or its Customers.	Y	
32	Assist individual departments and VITA-approved Users in lost or damaged file recovery from the Server backups by executing agreed recovery procedures or approved workarounds including defined Recovery Point Objectives (RPO) for the data.	Y	
33	Integrate with the MSI's SMS to provide VITA-approved Users with access to real-time system monitoring information via the Customer Portal with profiled access by VITA request (e.g. segregated by VITA Customer.)	Y	
34	Monitor and alert on thresholds (e.g. dataset or table space capacity events, full log files, file systems, etc.), and provide alerts to VITA and its Customers as specified in the SMM.	Y	
35	Provide support and management for existing Containers and/or Containerized Environments within the Commonwealth.	Y	
36	Support existing Cloud services which are being utilized by Customers but not approved through a formal VITA process. The support shall include remediation work to bring these services in-line with VITA Rules.	Y	
<b>9.2. Server Services</b>			
<b>9.2.1 General Services</b>			
1	Provision Virtual Servers as requested by VITA or VITA Customers.	Y	
2	Provide the maintenance, Patching, and Support of the Operating System.	Y	
3	Provide multi-tenant Software distribution Services to all Server platforms and enable VITA and VITA Customers to utilize these tools for Software distribution.		
4	Provide maintenance and Support of the Application/Web Server Software (e.g., WebSphere Application Server, WebSphere Application Server Network Deployment, IIS, JBoss Enterprise, WebLogic Application Server) as an add-on service when requested.	Y	
5	Provide the maintenance and Support of hypervisors.	Y	
6	Update and maintain shared-use file Server libraries of VITA's Software in accordance with the SMM.	Y	
7	Install and Support sufficient data Storage and processing capacity to facilitate the use of Server Applications Software.	Y	
8	Provide remote Software distribution to Servers.	Y	
9	Provide assistance in analyzing and correcting endpoint and/or Network Incidents and Problems that may be associated with Server	Y	
10	Provide node/host information to authorized VITA representatives or its agents, and check and reset ports.	Y	
11	Provide remote Software distribution.	Y	
12	Provide system administration and operational Support for high Availability clusters; multi-site high Availability clusters; Disaster Recovery; with automated and manual fail-over methods.	Y	
13	Provide technical Support for Server environments.	Y	
14	Install productivity tools/utilities, and perform all required operational modifications for the efficient and proper delivery of the Services.	Y	
15	Assign and initialize disk Storage volumes as required for performance of the Services.	Y	
16	Determine file, data set, and volume placement.	Y	

17	Install Software and perform monitoring and removal of malware programs from all Servers.	Y	
18	Perform Server administration functions, which include the development, establishment, Installation, and maintenance of:	Y	
18.1	Directories	Y	
18.2	Directory structures	Y	
18.3	Naming conventions	Y	
18.4	File structures	Y	
19	Create and maintain operational documentation for all Applications and User procedures that affect operations for VITA and VITA	Y	
20	Provide ability to integrate with new COV Services.	Y	
21	Enforce hardening standards as established by the Managed Security Services Provider and VITA Rules.	Y	
22	Provide external Internet based monitoring of DMZ Services (e.g., Web Servers).	Y	
<b>9.3 Database Services</b>			
	<p><i>SQL Server and Oracle Database Services on Virtual Servers. Supplier will be responsible for the administration of the Database Management System (e.g., maintenance plans, backup and recovery, clustering), Operating System and accompanying supporting tools.</i></p> <p><i>The Commonwealth currently owns Microsoft SQL Server licenses that are shared among Customers. For Oracle, the licenses are currently owned by VITA Customers.</i></p>		
1	Plan for Changes in the size of Databases that result from business growth and Project implementation based on information supplied by the MSI, VITA and its Customers, and review plans with the MSI and ITISP Governance on a regular basis for comment and approval.	Y	
2	Correct out-of-capacity situations caused by unusual activities in a timely manner (e.g., dataset or table space capacity events, full log	Y	
3	Proactively monitor and prevent out-of-capacity situations (e.g., dataset or table space capacity events, full log files.)	Y	
4	Develop, document, and maintain physical Database Support and management standards and procedures based on industry best practices as well as VITA and its Customers' needs.	Y	
5	Define Database creation, Configuration, Upgrade, Patching and Refresh requirements	Y	
6	Install, configure, maintain, and monitor Database management systems.	Y	
7	Create Databases and Database System Instances to Support VITA and its Customers.	Y	
8	Create scheduled and on-demand Database snapshots and clones.	Y	
9	Provide Databases with high availability as defined by business requirements.	Y	
10	Assist Customers with Database management system version upgrades and migrations.	Y	
11	In collaboration with the MSI, assist Customers with determining which Database Service best meets the Customer's requirements.	Y	
12	In collaboration with the MSI, assist Customers with determining the feasibility and implementation of high Availability Databases.	Y	
13	Provide data dictionary expertise, data assistance, data warehouse metadata definition, data mapping functions and creation of data cubes for VITA and eligible VITA Customers' Application developers.	Y	
14	Install, maintain, and Support Database Software.	Y	
15	Maintain Databases to meet the Service Levels and other performance standards, to maximize efficiency, and minimize outages.	Y	
16	Perform control functions to support existing Systems as of the Effective Date, as well as any planned new systems development.	Y	
17	Implement and administer appropriate Database management tools across all Database Instances (e.g., data masking tools, Redgate SQL Compare.)	Y	
18	Make performance metrics and historical data available for trending and reporting over a minimum of 6 months and be available via a	Y	
19	Provide Database management Support.	Y	
20	Test and implement Database environment Changes, as approved by VITA or VITA Customers.	Y	
21	Maintain consistent Database parameters and System settings across all like Instances.	Y	
22	Maintain Database consistency in accordance with the established Software Development Lifecycle.	Y	

23	Ensure Database consistency via tools to monitor, predict, and prevent Database corruption.	Y	
24	Open, track, and manage the Resolution of Database Problems.	Y	
25	Provide technical assistance, troubleshooting Support, and subject matter expertise to VITA, VITA Customer designee, and Third Party Vendor Support.	Y	
26	Monitor Database for Incidents and Problems and automatically generate Incidents and problems using the procedures, processes, and SMS defined in the SMM.	Y	
27	Provide customizable real-time notifications and alerts to the MSI and Customers via multiple modes of communication.	Y	
28	Perform Database administration backup & recovery, Security and Compliance.	Y	
29	Perform Database snapshots and clones at request of authorized Customers.	Y	
30	Maintain, operate, and Upgrade automated monitoring tools to monitor Database performance.	Y	
31	Employ Database performance analysis to confirm Database requirements in Support of Customer's business Systems.	Y	
32	Identify and Resolve locking conflicts, latch contention, rollback requirements, etc. for all Database Instances in coordination with VITA and eligible Customers' Application developers.	Y	
33	Define and execute Database performance and tuning scripts and keep Databases running at optimal performance for the Commonwealth's workloads	Y	
34	Perform Database reorganizations to optimize performance when required via established thresholds or Customer requests.	Y	
35	Execute Database System Configuration Changes, Upgrades and Patches in accordance with the SMM.	Y	
36	Maintain documentation for Database Instance parameters and System settings.	Y	
37	Perform shutdowns and restarts for Database management Systems, Instances, and individual Databases as requested by the MSI or	Y	
38	Maintain, Update, and implement Database archive Processes and Procedures, as defined in the SMM, to recover from an outage or corruption to meet established SLAs in order to meet VITA's business requirements.	Y	
39	Execute VITA and its Customers' Database backup schedules, retention periods, and levels (i.e. full, incremental, or differential)	Y	
40	Exercise Database restores from Database exports, dumps, backups, flat files, secondary Databases, and disk based snapshots.	Y	
41	Provide granular restoration options to include the Server, Instance, Database, table, and row levels at Customer defined recovery points.	Y	
42	Provide Security administration including Service Requests, managing role and End-User Database permissions in accordance with the SMM, which may include Customer-specific policies.	Y	
43	Execute authorization requirements as defined by VITA and its Customers (e.g., Users, roles, schemas.)	Y	
44	Provide Database management encryption for the entire system or subcomponents as requested by VITA or its Customers.	Y	
45	Provide an interface for VITA and its Customers to delegate Database Security functions	Y	
<b>9.4 Storage Services</b>			
<i>Supplier is responsible for providing Multi-tenant multi-tiered Storage Services to VITA and VITA Customers. Supplier's Storage Support responsibilities include all levels and types of Cloud Storage. The environment requires multiple levels of speed, redundancy, scalability, Availability, and Security.</i>			
<b>9.4.1 Storage Management</b>			
1	Remain current in the knowledge and use of data Storage technology and management products and provide new emerging Storage	Y	
2	Provide encryption at rest Services for all tiers of Storage.	Y	
3	Perform online Storage tuning.	Y	
4	Provide event, warning, alert, and alarm processing and management.	Y	
5	Resolve all event, warning, alert, and alarm messages.	Y	
6	Utilize and Support Incident and Problem Management in accordance with the SMM.	Y	
7	Provide Storage and Backup infrastructure Configuration maintenance.	Y	
8	Provide improvement or remedial activities in operational processes in accordance with the SMM.	Y	

9	Assign and initialize Storage volumes as required.	Y	
10	Manage the archiving of inactive files and report on Storage directories for review by VITA and VITA Customers.	Y	
11	Conduct routine monitoring using Software tools to measure the efficiency of online storage access, and take corrective action as needed (including performance adjustments to Equipment and Software, or file placement as required to improve service).	Y	
12	Provide multiple tiers of Storage to Support differing performance needs.	Y	
13	Provide multi-site buffered replicated Storage for all tiers of Storage.	Y	
14	Provide multi-site active-active storage to support multi-site highly available clustered Databases.	Y	
15	Maintain and improve storage resource efficiency and space utilization requirements.	Y	
16	Support Storage for high-speed relational and non-relational Databases, data-marts and data warehouses utilizing Oracle and Microsoft SQL and other technologies.	Y	
17	Create and keep up to date the backup and Storage procedures defined in the SMM.	Y	
18	Provide data migration services from existing to new backup and storage service platforms including migration of existing Access Control Lists (ACLs) if applicable.	Y	
19	Provide secure, durable data sharing services between heterogeneous nodes and platforms.	Y	
20	Monitor, maintain and Report on User directories for file activity and inactivity.	Y	
21	Provide online Storage compression as needed.	Y	
22	Provide automated de-duplication of data.	Y	
23	Provide data migration and archive management at both the User level and array level.	Y	
24	Provide documentation Support and maintenance.	Y	
25	Monitor and control Storage performance according to SMM.	Y	
<b>9.4.2 Backup and Recovery Services</b>			
1	Assume responsibility for compliance with VITA's Data Availability Standard.	Y	
<b>9.4.3 Provisioning and De-Provisioning of Storage</b>			
1	Provide mechanism for Customers to expand or remove Storage Services as needed to meet requirements.	Y	
2	Provide an automated workflow for Storage Service provisioning and de-provisioning that integrates with the MSI Service Management	Y	
3	Supplier will adhere to all VITA and VITA Customer Security Policies regarding the destruction of data after de-provisioning request is	Y	
4	Provide capability to provision Storage that allows VITA and VITA Customers to pay for Storage consumed instead of Storage allocated.	Y	
5	Wipe and erase the data and Configuration information resident in Storage, Storage components, and/or Devices complying with VITA Rules prior to removing or reallocating.	Y	
<b>9.4.4 Security and Data Management</b>			
1	Comply with VITA Rules including Security, data and records management, and electronic records and data archiving.	Y	
2	Provide Data management Support including:	Y	
2.1	Leverage industry best practices for the management and organization of Customer data.	Y	
2.2	Develop and document in the SMM procedures for performing Storage and Data management and archive procedures that meet requirements and conform to defined policies.	Y	
2.3	Provide a solution that allows for the archiving of data based upon various criteria such as last accessed date.	Y	
2.4	Provide access to data and backups that allows for cost effective Storage.	Y	
2.5	Design, document in the SMM, and implement a data lifecycle management plan based on VITA and VITA Customer (e.g., Library of Virginia) requirements or regulations.	Y	
2.6	Support data type classification requirements and labeling (e.g., FTI, PCI) in accordance with VITA Rules.	Y	
2.7	Provide expedited Support for e-discovery and special legal or legislative requests of data (e.g., FOIA).	Y	

<b>9.5 Network Services Associated with Server/Platform/Storage Services</b>		
	<p><i>Supplier responsibilities related to Cloud Network Services includes administration of Network components within any Cloud Service Provider.</i></p> <p><i>The Commonwealth hosts a multi-tenant Network where each Customer has access to their own secure segmented Networks, segmented Virtual Routing and Forwarding VRF tables, a shared Network for shared Services, and a DMZ for Internet Services. While it is one Commonwealth Network, each Customer is logically isolated from other Agencies.</i></p> <p><i>The scope is everything up to the core switch within Cloud Service Provider which includes:</i></p> <ul style="list-style-type: none"> <li>• <i>Local Area Network Services</i></li> <li>• <i>Networked Appliance Services</i></li> <li>• <i>Integrate with MSS supplier for Network Security Services</i></li> <li>• <i>Load Balancing Services</i></li> <li>• <i>Private Network Services</i></li> <li>• <i>Integrate with SSDC supplier for Network Time Services</i></li> <li>• <i>Integrate with SSDC supplier for IP address management Services</i></li> <li>• <i>Cloud Network Performance monitoring and management Services</i></li> </ul>	
<b>9.5.1 General Requirements</b>		
1	Act as a single point of contact for the management of the Cloud Network, including assisting the MSI and other Service Tower Suppliers.	Y
2	In collaboration with the MSI, provide VITA-approved Users, other Service Tower Suppliers and designated Third Party Vendors with technical support and advice regarding the use and functionality of Cloud Network Services.	Y
3	Provide highly available redundant Network load balancing Services.	Y
4	Perform load balancing as required by Customers.	Y
4.1	Provide Support for complex load balancing rules. (e.g., Session State, Source IP, Least Connections, round-robin balance, weighted load distribution)	Y
4.2	Provide Support for two-arm (in-line), one-arm, and direct server response load balancing.	Y
4.3	Provide Support for load balancing SSL termination and pass thru of SSL.	Y
4.4	Implement and maintain the load balancing SSL certificates mandated by Customer.	Y
5	Maintain and Install upgrades, configure and fine-tune Cloud Network operating Software in accordance with SMM.	Y
6	Administer all Cloud Network required activities, including processing change requests.	Y
7	Provide a fully redundant Network based Architecture (e.g., dynamic routing)	Y
8	Provide for least latency based route selection, where traffic is routed to the 'best' Network gateway	Y
9	Assume all aspects of the Cloud Network Services in accordance with VITA Rules and the SMM, including:	Y
9.1	Design criteria and standards	Y
9.2	Escalation procedures	Y
9.3	Service acceptance procedures	Y
9.4	Topology documentation	Y
9.5	Contact information	Y
9.6	System inventories	Y

9.7	Disaster Recovery Plans (including Technical Recovery Guides)	Y	
10	Assume documented operations Procedures and Services.	Y	
11	Maintain Site logs in a centralized location in accordance with VITA Rules and the SMM.	Y	
12	Provide Site logs in a portable, industry-standard format in accordance with VITA Rules and the SMM.	Y	
13	Provide a mechanism for Network segregation internally within the service to enable consumer systems to be segmented according to VITA's criteria of data classification or Security zones.	Y	
14	Provide a mechanism for Customers to define firewall rules for communications between the different Network segments.	Y	
<b>9.5.2 Planning and Design Services</b>			
1	Collaborate with the MSI, VITA, and the ITISP Governance to analyze the Cloud Network Service needs.	Y	
2	As directed by the MSI, provide programming, engineering, and design functions for any proposal requested by VITA for new or changes to the existing Cloud Network Service environment.	Y	
3	Provide flexible Network solutions.	Y	
4	Continue to support the following components:	Y	
4.1	Overall Network Topology, including the physical and logical layout of the Cloud Network.	Y	
4.2	IP addressing and Device/Host naming schemas.	Y	
4.3	Security compliance.	Y	
4.4	Optimal communications protocols within the Cloud Data Center LANs as necessary to satisfy VITA's and VITA Customers' business and operational requirements as they evolve.	Y	
4.5	Network Device.	Y	
4.6	Network Software.	Y	
4.7	Network Appliances.	Y	
4.8	Transport Services.	Y	
4.9	Network bandwidth and volume assumptions and projections.	Y	
4.10	Expected performance and Quality of Service (QoS) based on designs and plans, and minimum performance and QoS expectations.	Y	
4.11	Expected Availability, based on designs and plans for redundancy, and minimum availability expectations.	Y	
5	Design, implement, and maintain Network Devices to eliminate single points of failure (e.g., routers, switches, load balancers).	Y	
6	Provide Network prioritization of traffic. (i.e., QoS)	Y	
7	Prevent broadcast congestion and outages.	Y	
8	Design and implement segmentation of traffic, and design features to sufficiently control and contain traffic levels.	Y	
9	Design and implement sufficient redundancy and alternative routing to meet the Service Levels and VITA and VITA Customers' Security and Service Continuity requirements.	Y	
10	Work cooperatively with other Integrated Suppliers, Third Party Vendors, VITA, and ITISP Governance to facilitate effective planning and design of the VITA Network.	Y	
<b>9.5.3 Operations and Maintenance</b>			
1	Install, change, disconnect or remove Cloud Network Devices and related software and configurations to meet VITA's and VITA Customers' business and Application requirements in accordance with the processes and procedures in the SMM.	Y	
2	Implement Cloud Network connections for all VITA-approved Users, designated Devices and Applications, other VITA Suppliers and designated Third Party Vendors, as required.	Y	
3	Implement Cloud Network Segments as requested.	Y	
4	Implement load balancing Configurations as requested.	Y	
5	Assign and Implement IP address ranges as requested.	Y	

6	Implement routing and filtering as requested.	Y	
7	Maintain Networking environment and upgrade Cloud Network Services as required to meet VITA and VITA Customer business and Application requirements, and in compliance with approved Refresh targets.	Y	
8	Plan, Install, operate, and maintain all applicable Cloud Network Services/Devices.	Y	
9	Assist the MSI, Customers and authorized Third Party Vendors with end-to-end bandwidth analysis as requested.	Y	
10	Provide secure, encrypted Connectivity for Users of Cloud Network Services in accordance with VITA Rules and the SMM.	Y	
11	Employ appropriate encryption measures.	Y	
<b>9.5.4 Monitoring</b>			
1	Configure, Implement, and Maintain the appropriate Cloud Network Devices monitoring.	Y	
2	Monitor and manage continuous performance of Cloud Network Systems/Devices.	Y	
3	Use intelligent Network Devices, Systems, and Tools to effectively monitor Cloud Networks remotely.	Y	
4	Test Cloud Network Devices after implementation to include remote monitoring through agents and monitoring systems.	Y	
5	Monitor alarms sent by Customer Network Systems; perform emergency and routine service in response to critical and non-critical	Y	
6	Integrate alerting into Commonwealth Joint Operations Center provided by the MSI.	Y	
7	Integrate logging into Commonwealth Security Information and Event Management (SIEM).	Y	
8	Provide automatic notification of issues identified by the monitoring solution in accordance with VITA Rules and the SMM.	Y	
<b>9.5.5 Network-based Appliance Services</b>			
1	Provision, Install, operate, Support, and manage multi-tenant segmented Network based Appliances as directed by the MSI.	Y	
2	Provide and support the tools that integrate with the MSI's SMS and that provide Customers with access to User information and administration capabilities as required.	Y	
3	Provide for the partitioning of the Service such that multiple Customers can securely share the use of Network Appliances, including the Support of multiple organizations and sub- organizations.	Y	
4	Provide Reports on the usage of Network Appliances in accordance with the SMM.	Y	
5	Provide additional detailed Reporting for auditing and compliance.	Y	
6	Provide all technical system Support and Reporting for operations including:	Y	
6.1	Storage management for all media	Y	
6.2	System programming	Y	
6.3	Capacity planning	Y	
6.4	Performance analysis and tuning	Y	
7	Install and maintain all system Software products.	Y	
8	Develop and Install productivity tools/utilities, and perform all required operational modifications for the efficient and proper delivery of the Services.	Y	
9	Provide regular monitoring and Reporting of performance, utilization, and efficiency in accordance with VITA Rules and the SMM.	Y	
10	As directed by the MSI, provide technical advice and Support (e.g. Architecture) to VITA, VITA Customers, other Service Tower Suppliers and specific Third Party Vendors, as required.	Y	
11	Supplier responsibilities include providing, Installing and utilizing tools and processes to allow automated and remote systems management of Network Appliances. The outcome of all activities will be made available to VITA and VITA Customers upon request via the MSI SMS. Such tools and processes will include:	Y	
11.1	Administration, management and Configuration	Y	
11.2	License management tools	Y	
11.3	Performance measurement and tuning	Y	

11.4	System monitoring and controls	Y	
11.5	Disaster Recovery, Backup/Recovery, and Business Continuity	Y	
11.6	Automatic alerting to Support automated Incident creation and notification of affected VITA Customer	Y	
11.7	Integration into SIEM and SMS tools and MSI Joint Operations Center	Y	
11.8	Configuration discovery	Y	
11.9	Patch management	Y	
<b>9.6 Security Functions</b>			
<b>9.6.1 General Integration</b>			
1	Coordinate with Managed Security Supplier via the MSI to support Managed Security platform toolset within the Managed Environment.	Y	
2	Install, operate, Configure, Support, and manage Managed Security platform toolset in the environment in accordance with the SMM.	Y	
3	Communicate and report any Intrusion detected in the environment in accordance with the SMM.	Y	
<b>9.6.2 Data Security</b>			
	<i>Data Security includes Security controls that are intended to protect Commonwealth data. Data may traverse or be stored within the environment and outside the environment. The controls included in this section focus on protecting the data itself with controls such as</i>		
1	Provide enhanced Security Services for specific Database Instances to minimize Security concerns due to out of Support Database	Y	
2	Implement the EDS solution to ensure that it does not modify the monitored Databases and will have minimal impact on Database	Y	
3	Perform EDS Configuration Updates in accordance with the SMM.	Y	
<b>9.7 OCI Specific Assumed Services</b>			
	<i>The following list of OCI specific services and activities should be used by Suppliers as a view of the current services being provided for one Agency in the Commonwealth. These services may not represent all OCI tenets in the Commonwealth. These services are subject to change and all services will need to be incorporated into the Supplier's final solution. More information regarding this tenet can be found in Environment Overview _ (DOA Cardinal Environment).</i>		NTT DATA is not providing OCI services
	<i>Note: This section shall only be complete by Offerors who are submitting a response for OCI. This section shall be left intentionally blank if the Offeror is responding to Azure or GCP</i>		
1	Own all OCI Console standard functions including but not limited to creation and maintenance of subnets, security and role definitions, routing rules, network security groups, and security lists.		
2	Complete monthly Compute Windows patching for Cardinal/DOA VMs. Development and Test VMs are typically patched the 3rd Sunday morning and Production VMs are typically patched the 4th Sunday of the month excluding VITA change freezes.		
3	Complete monthly Compute Linux patching for Cardinal/DOA VMs. Development and Test VMs are typically patched the 1st Sunday morning and Production VMs are typically patched the 2nd Sunday of the month excluding VITA change freezes.		
4	Coordinate monthly ExaData Dom0 and Storage Cell patching with Oracle's patching group. Development & Test ExaData systems are typically patched the 1st Sunday of the month and Production VMs are typically patched the 2nd Sunday of the month but may be adjusted based on the business calendar (i.e. no Production patching during the first half of May during the Open Enrollment period)		
5	Complete all standard Windows and Linux OS admin responsibilities for Compute Windows, Compute Linux. Continue to share responsibilities for OS admin functions on the ExaData Linux VMs with the Cardinal DOA team as has been in place with current VITA provider. Cardinal will continue to complete DomU patching given its close dependencies on Oracle Grid and database patching.		
6	Maintain and support the LDAP integration configured that allows AD accounts and credentials to be used to access all Cardinal Windows and Linux VMs.		
7	Maintain and support the current Active Directory, Domain Controller, DNS, and conditional DNS configurations in OCI.		
8	Coordinate with VITA's OKTA support vendor to maintain the integration in place that allows Okta accounts to be used to access the OCI		

9	Support, maintain, and upgrade Cardinal/DOAs F5 LoadBalancer configuration.		
10	Provide a named resource who will serve as the Coordinate for all Cardinal/DOA work requests and tickets for the supplier. This resource will be expected to conduct weekly checkpoint meetings for Cardinal/DOA management and will be the escalation point of conduct.		
11	Continue to support Cardinal DOA's Enhanced Support Services (ESS) where Supplier resources charge hours above and beyond standard support for tasks and tickets requested by Cardinal/DOA without the need for an RFS.		
12	Support any and all requests for information during Audits of Cardinal/DOA by APA, VITA, or other groups.		
13	Participate in annual Disaster Recovery (DR) exercises for Cardinal DOA. Cardinal drives the annual tests but the Supplier has a small number of Defined Tasks as noted in Cardinal's DR runbook.		
14	Join and participate in existing TEAMS chats with Cardinal DOA for standard support needs as well as triage for Production issues.		
15	Support the ability to provision all current and future Compute shapes and ExaData system options in OCI Gov Cloud.		
16	Conduct a quarterly meeting with Cardinal DOA (and other agencies in OCI is do desired) summarizing new features of OCI Gov Cloud that have been released as well as the roadmap for any major planned changes within VITA tenancy (e.g. Need for an update to the Dynamic Routing Gateway)		
<b>9.8 Azure Specific Assumed Services</b>			
<p><i>The following list of Azure specific services and activities should be used by Suppliers as a view of the current services being provided for one Agency in the Commonwealth. These services may not represent all Azure tenets in the Commonwealth. These services are subject to change and all services will need to be incorporated into the Supplier's final solution. More information regarding this environment can be found in Environment Overview _ (VDOT Azure Environment).</i></p> <p><i>Note: This section shall only be complete by Offerors who are submitting a response for Azure. This section shall be left intentionally blank if the Offeror is responding to OCI or GCP</i></p>			
1	Support all Management Groups and hierarchy in line with Microsoft CAF (Cloud Adoption Framework)	Y	
2	Support Subscriptions provided to VDOT and Subscriptions proposed as part of VDOT's POC	Y	
3	Support Datalake environment with all supported components	Y	
4	Support VNET infrastructure and supporting components (Private endpoints, NICs, Subnets, Peering, Route Tables, Load Balancers, PIPs, etc.), with connection to express route (Verizon SCI) back to QTS Data center	Y	
5	Support all Azure native services. Including, but not limited too, Storage Accounts, VMs (and supporting components), Web Apps, Azure Data Factory, SQL DB, SQL Managed Instance, Function Apps, Databricks, Key Vaults, Logic Apps, Cognitive Services, Synapse, QnA maker.	Y	
6	Support Agency(s) with Azure DNS services for on prem DNS resolution of Azure Services that are private.	Y	
7	Work with Microsoft to implement proven practices and guidance for Agencies to leverage in adopting and migrating to Azure.	Y	
8	Work with Agency to support and manage all aspects of Azure Cloud	Y	
9	Manage Databricks account and workspaces at the top level including Unity Catalog, policies, and AAD integration	Y	
10	Support all Azure Active Directory(AAD) related components including, but not limited to: enterprise applications, application registrations, enterprise-level roles, and on-prem AD synchronization.	Y	
<b>9.9 GCP Specific Assumed Services</b>			
<p><i>The following list of GCP specific services and activities should be used by Suppliers as a view of the current services being provided. These services are not currently in the VITA environment at the time of solicitation posting. The Supplier may be responsible for bringing these services into the VITA environment and conforming, as necessary, to VITA Rules. These services are subject to change and all services will need to be incorporated into the Supplier's final solution. More information regarding this environment can be found in Environment Overview _ (VDH GCP Environment).</i></p> <p><i>Note: This section shall only be complete by Offerors who are submitting a response for GCP. This section shall be left intentionally blank</i></p>			NTT DATA is not providing GCP services

VA-240920-NTT 02.1 Exhibit - Description of Services - Managed Public Cloud Services

1	Support and maintain all AD-based groups and AD-to-Google identity synchronization		
2	Support and maintain existing serverless technology implementations and those in-progress		
3	Support and maintain existing tags / labels and current naming standards / nomenclature		
4	Support and assist agency-planned effort to set up access to specific data items by non-COV entities, including the use of Identity Aware Proxy for provisioning non-COV user accounts and permissions		
5	Support agency implementation of data governance infrastructure and existing architecture		
6	Support use of IAM by Agency staff to provision access and precise permissions (limited to specific staff only)		
7	Support existing and planned automatic provisioning and scale-up / scale-down of resources (cluster, compute, storage, memory)		
8	Support existing custom-built applications and systems including Call Center AI, Vaccine Management		
9	Support ongoing development of custom-built Data Governance platform and work with vendor performing this development		
10	Support and maintain existing connections and APIs from third-party data tools including Tableau, ArcGIS, Posit (formerly R), SAS, SPSS,		
11	Support and maintain existing project / folder architecture		
12	Support continued access to billing information, reports, and triggered budget notifications		
13	Support current in-use components including: BigQuery, GCS, BigTable, DataPlex, Data Fusion, IAM, VPCs, VertexAI, Jupyter notebooks		
14	Support extract of data into MS Excel (specifically)		
15	Support creation of datasets, data tables / views, stored procedures / processing capability, and automated routines to include data ingestion from multiple sources, both COV and non-COV		
16	Support ability of VDH staff to create and implement new projects and folders		
17	Support VDH staff linking new projects to billing account and enabling features / components within those projects (note: VDH is responsible for vetting and allowing staff to perform these functions - this is not a free-for-all)		
18	Support VDH staff ability to modify and move projects as needed (same restriction as above)		
19	Support Terraform code repos, existing development and QA practices and procedures, existing and underway IAC implementations, and code promotion processes and automation		
20	Support ability to use Google Cloud Console in addition to native UI		
21	Support existing log sinks, Splunk connections (if in place), and any other VDH-defined logging requirements		
22	Liaise with Google Professional Services, Technical Services, and other representatives as required to assist in troubleshooting issues		
23	Support existing Amazon S3 Bucket, Azure, COV network drive, SQL Server, Oracle, and / or Federal or State government connectivity, and data exchange across / between these entities		

VA-240920-NTT: Managed Public Cloud Services

Ref #	Requirement	Comply (Y/N)	Supplier Response
	<b>10.0 Additional (Optional) Services</b>		
	<i>The following list of services shall be considered Additional (Optional) Services. A supplier's ability to provide these services will not be evaluated by VITA as part of this RFP.</i>		
	<i>The MCS provider may be required to operate independent of the MSI CBTI at VITA's discretion in response to various situations. A number of MCS Additional Services may be activated in these situations.</i>		
	<i>The MCS provider may be directed by VITA to:</i> - Enable its Cloud Management Platform (CMP) as an enhanced service for direct VITA and Agency use as the single pane of glass. - Enable its role in managing any or all of Cloud Service Catalog, Cloud Governance, Financial Management, Service Asset Configuration Management, Reporting, and managing the Tagging Strategy.		
1	<i>If any Additional Services are requested by VITA then, the supplier may be required to:</i>		
1.1	Provided a transitional implementation period to allow for implementation planning, acceptance test planning, and acceptance testing by VITA, all of which is to be approved by VITA prior to implementation	Y	
1.2	A complete implementation acceptance test will be performed by VITA using the approved acceptance test plan, during which MCS must demonstrate "pass" conditions prior to receiving associated milestone	Y	
1.3	Maintain a common set of capabilities across its in-scope CSPs for the duration of the enhanced agreement.	Y	
1.4	Coordinate with VITA to ensure timely communication to VITA Customers of available training opportunities and events in relation to any Enhanced Services VITA has exercised an option to commence.	Y	
1.5	Organize a Service Management Manual chapter of documents, subject to VITA's approval in relation to any Enhanced Services VITA has exercised an option to commence.	Y	
1.6	Produce the named SMM chapter documents as approved by VITA in relation to any Enhanced Services VITA has exercised an option to commence.	Y	
1.7	Produce Keystone Edge based knowledge articles to be included in the MSI's Knowledge Base in relation to any Enhanced Services VITA has exercised an option to commence.	Y	
1.8	Collect and fulfill requests from the VITA Customer users to access cloud services or deploy cloud resources.	Y	
2	<i>Supplier's enhanced Cloud Management Platform (CMP) responsibilities may include:</i>		
2.1	Tools that will enable Agency Users to move workloads across CSP tenants. Helps adjust transition among CSP suppliers in the infrastructure without complications.	Y	
2.2	A management portal user interface (UI) deployed, maintained, and enhanced at least monthly for all stakeholders to access with role-based rights.	Y	
2.3	A cloud shell /CLI to pull required details for oversight compliance ease/speed.	Y	
2.4	Perform Consolidated billing (across multiple accounts and/or multiple cloud providers)	Y	
2.5	Perform event and performance monitoring and analytics, with dashboard reporting	Y	
2.6	Enable Agency Users serving as Agency cloud managers to provision and orchestrate cloud resources and	Y	
2.7	Enable Cloud service expense management.	Y	
2.8	Enable Resource and service optimization.	Y	
2.9	Provide an API through which customers can integrate their agency-based tools for analytics.	Y	
2.10	Identity and access integration with VITA identity services.	Y	
2.11	Identity and access integration with each hyperscale cloud provider's service.	Y	
2.12	Packaging and templating of workloads.	Y	
2.13	Integrates Approval workflows in the CMP that support and continually improves service management processes in the VITA SMM (ITIL use cases).	Y	
2.14	Enables Hybrid IT (integrated management of on-premises resources, such as from VMware or VITA private cloud data center environment).	Y	
2.15	Multicloud (all clouds under management can at least be viewed in aggregate).	Y	
2.16	Enable Application performance monitoring.	Y	
2.17	Enable Migration process support and tool integration.	Y	
2.18	Enables management of Disaster recovery and data protection.	Y	
2.19	Minimize ingress and egress data flows and costs in the environment.	Y	
3	<i>The Supplier's Enhanced Service Catalog Services may include:</i>		
	<i>Note: The Cloud Service catalog is the central repository for the ordering of cloud services by VITA's customers. In addition to listing the most commonly used and available product offerings, the Service Catalog provides the filtering of appropriate and allowed options for specific services, and ensures only authorized purchases are provisioned by incorporating appropriate approval workflows.</i>		
3.1	Provide pre-developed catalog items continued in the platform for inclusion in the Enterprise Service	Y	
3.2	Integration with the MSI provided service catalog to support utilization of approval workflows already developed for VITA customers.	Y	
3.3	Develop catalog items for the most frequently used cloud offerings to facilitate ordering and rapid	Y	
3.4	Automate provisioning as appropriate to expedite delivery of cloud services to VITA's customers including the provisioning of approved "gold images".	Y	

3.5	When automated provisioning is not possible or practical due to complexity of the end user's request, the MCS shall forward the request via an appropriate workflow to the Cloud Services Tower Supplier for manual provisioning into the environment.	Y	
3.6	Provide a ROI calculator and training on use of the calculator for use by VITA, Cloud Service Tower, MSI, and Agencies for use when planning their cloud adoption.	Y	
4	<i>The Supplier's enhanced MCS Financial Management may include:</i>  <i>Note: VITA requires the ability to view total VITA Cloud spend in various dimensions; by CSP, VITA Customer, Project, and Resource Tag and reconcile those back to the VITA Customer. The MCS shall establish and execute processes to collect, analyze, and identify actual CSP usage that supports the allocation of actual costs back to the VITA Customers. The MCS's process and procedures will consolidate, organize, and present CSP billing data organized by VITA Customer and CSP resource (e.g. Resource Tag) or as needed by VITA</i>		
4.1	Provide a consolidated report that allows VITA to view total spend by CSP, VITA Customer, Project, Resource	Y	
4.2	Provide backup and supporting information to support invoice reconciliation and resolution of billing	Y	
4.3	Provide consolidated billing reporting services for all CSP Master and Member accounts. This capability shall be made available upon issuance of the first invoice under the contract.	Y	
4.4	Integrate financials with the MSI ITSM System for consolidated billing and reporting.	Y	
5	<i>The Supplier's Enhanced Cloud Service Asset Configuration Management may include:</i>		
5.1	Updates to the CMDB upon an Agency provisioning and de-provisioning requests to permanently stand down cloud resources or when approved changes are made to the CI through the Enterprise Change	Y	
6	<i>The Supplier's Enhanced Reporting requirements may include:</i>  <i>Note: VITA has a continuing requirement for reporting of systems that a Supplier manages against VITA stated performance objectives, including but not limited to metrics for components in areas including availability, performance, capacity and utilization, incidents and events, and problem management. VITA expects a flexible reporting capability that is available to both CIO, designee, and VITA Customers for producing standardized reports and allows for further development of ad hoc reports on selected service metrics, logs, or account utilization. Reports shall be available at agreed upon schedules and intervals to both CIO, designee, and VITA Customers. VITA will retain unlimited access to all reports via dashboards, monitoring tools, or other agreed on methods or systems for disseminating collected information for</i>		
6.1	Provide necessary information to VITA to comply with Commonwealth's mandated reporting requirements.	Y	
6.2	Notify VITA and the VITA Customer when cloud usage hits the 75% threshold or when there are only 3 months of cloud services available based on cloud usage.	Y	
6.3	Provide reports on SLA performance of help desk ticket remediation and trends.	Y	
6.4	Provide SLA metric results in accordance with SLA reporting requirements established by the MSI.	Y	
6.5	Support VITA in providing, as required, reports supporting budget formulation exercises.	Y	
6.6	Participate in briefings to the VITA Cloud Service Owners and CIO staff and shall develop Status Reports for those meetings.	Y	
6.7	Develop and maintain an SLA Performance dashboard.	Y	
7	<i>The Supplier's Enhanced monitoring and reporting dashboard(s) may be required to:</i>		
7.1	Administer a VITA approved monitoring tool for key cloud services metrics (e.g., site availability, load time, user authentication, server and application events, web, and database services).	Y	
7.2	Identify to VITA for approval the monitoring tool(s) and indicate if the monitoring tool(s) are CSP native, third party, or custom developed.	Y	
7.3	Provide customized and comprehensive dashboards from its toolset, such as provisioned assets, performance metrics for VITA Cloud assets, near-real time cloud spend metrics and reports, security and compliance metrics, and general up/down status of provisioned assets.	Y	
7.4	Provide and update incident management, change management, project management, uptime, responsiveness, and general health dashboards of key infrastructure components to validate service level	Y	
	Answering technical queries and assisting Users.	Y	
7.5	Track and report near-real-time metrics in a performance dashboard containing but not limited to the following data: Server Uptime CPU utilization Memory utilization Disk utilization Data Network egress utilization	Y	
8	<i>The Suppliers enhanced Tagging Strategy Management may be required to:</i>  <i>A defined cloud tagging strategy is essential to tracking, reporting, and billing for cloud assets. The tagging strategy provides the consistent data structure to allow for a true Enterprise view to cloud spend at an appropriate level. Any cloud assets deployed without using the Enterprise standard cloud tagging strategy may not be accounted for in an appropriate unified view, or may require significant manual effort to interface with cost and performance reporting. This is also applicable to security and logging events per</i>		
8.1	Provide an appropriate cloud tagging strategy to VITA for review and feedback.	Y	

8.2	Work with VITA to accommodate reasonable changes to support VITA billing practices as long as the requested changes are in alignment with industry best practices.	Y	
8.3	Provide a documented tagging strategy after incorporating VITA and Agency feedback	Y	
8.4	Implement for security and logging events, per user, group, business, Agency, etc.	Y	
8.5	Implement the approved tagging standard in catalog CIs that have been provisioned through the MCS.	Y	
8.6	Provisions for allowing Agencies to create, use, modify, and delete their own tags.	Y	
9	Provide training and support to Agency stakeholders to help them understand MCS-performed analytics for managing cloud consumption decisions.	Y	
10	Provisioning and orchestration: The cloud management tasks used to create, modify, and delete resources, and to orchestrate complex deployment and management operations.	Y	
11	Cloud migration, backup, and disaster recovery (DR): The ability to replicate data to migrate workload, implement business continuity or DR architectures, or to protect data against accidental deletion or malicious activity. The Supplier maybe expected to develop disaster recovery and backup plans that are	Y	
12	Identity, security, risk, and compliance: Manage and secure access to cloud services as well as enforce a security configuration baseline.	Y	
13	Consolidate cryptographic key management in its toolset in a manner that ensures VITA and Agencies have control over access to its data in accordance with VITA Rules.	Y	

VA-240920-NTT: Managed Public Cloud Services

Ref #	Requirement	Adhere	Inform	Create	Comply (Y/N)
	<p><b>11.0 SMM RESPONSIBILITIES</b></p> <p><i>The Service Management Manual serves as a Enterprise level library of common documents shared among the Integrated Suppliers within VITA's managed environment. All Integrated Suppliers will operate in accordance with and be subject to the terms therein. Suppliers shall reference <u>MSA 1.4.2 (Service Management Manual)</u> for additional information regarding the SMMs.</i></p> <p><i>The contents of this tab outlines the Service Management Manual (SMM) and the responsibility of the Supplier. The SMMs are broken up into three (3) categories.</i></p> <p><i>Adhere: Suppliers shall conform and adhere to these SMMs in order to operate within VITA's managed environment.</i></p> <p><i>Note: Suppliers may request all "Adhere" SMMs from the Single Point of Contact for this RFP.</i></p> <p><i>Inform: These SMMs are for informational purposes. Suppliers may need to interface with other Suppliers and need to be aware of their contents.</i></p> <p><i>Create: Suppliers shall create SMM documentation to align to the section topic prior to the Commencement date. Suppliers shall be responsible for updating their submitted SMMs in accordance with <b>Exhibit 3.4 (Report Matrix)</b>.</i></p> <p><i>An "X" indicates the level of responsibility a new supplier shall have within VITA's</i></p>				
	<p><i>Instructions: Supplier should enter a "Y" (Yes) or "N" (No) in Column F to indicate if it complies with the SMM as written.</i></p> <p><i>Where a cell is shaded under the "Comply (Y/N)" column, no response is required.</i></p> <p><i>If Supplier does not comply with an "Adhere" SMM exactly as written, Supplier must enter an "N" in the "Comply (Y/N)" Column F and provide Supplier's proposed changes to the SMM by utilizing the table provided in <b>Exhibit 2.3.1 (Solution - Managed Public Cloud Services)</b>. Supplier should make proposed changes to text using "revisions" or some other method to clearly indicate</i></p>				
1.0	SMM Contents				
1.1	Purpose	X			Y
1.2	SMM Document Management	X			Y
2.0	Organization, Governance, and Contact Information		X		
2.1	WMM Case Management	X			Y

VA-240920-NTT 02.1 Exhibit - Description of Services - Managed Public Cloud Services

2.2.5	Governance				
2.2.5.1	PAG Charter	X			Y
2.2.5.2	Technical Review Board Charter	X			Y
2.2.5.3	Change Advisory Board Charter	X			Y
2.2.5.4	Platform Service Delivery Forum Charter	X			Y
2.2.5.5	Service Portfolio Life Cycle Management Charter	X			Y
2.2.5.6	Program Management Forum Charter	X			Y
2.2.5.7	Service Integration and Interoperability Forum Charter	X			Y
2.2.5.8	Architecture and Innovation Forum Charter	X			Y
2.2.5.9	IT Financial Management Forum Charter	X			Y
2.2.5.10	Cyber Security Operations Forum Charter	X			Y
2.2.5.11	IT Service Continuity Management Forum Charter	X			Y
2.2.5.12	Service Tower Forum Charter	X			Y
2.2.5.13	Customer Operations Meetings Charter	X			Y
2.2.5.13a	Customer Relationship Management Forum Charter	X			Y
2.3+	STS XX Organization				
2.4	STS MF Organization Overview (Peraton)		X		
2.6	STS MSS - ATOS Organization		X		
2.7	STS SSDC Organization		X		
2.8	STS Managed Print Xerox Organization Overview Information		X		
2.9	STS EUC Organization Overview		X		
2.10	STS VRZN Organization Overview		X		
2.11	NTT Messaging Services Organization Overview		X		
2.1X	MCS Services Organization Overview			X	Y
3.0	Service Tower Supplier Implementation				
3.1	Deliverable Management	X			Y
4.0	IT Service Lifecycle Processes				
4.1	Common IT Service Lifecycle Processes				
4.1.1.1	Program Management Office	X			Y
4.1.1.2	Project Portfolio Management	X			Y
4.1.1.4	Ongoing Programs	X			Y
4.1.1.6	Resource Management	X			Y
4.1.1.8	Program Quality Management	X			Y
4.1.2	Service Strategy	X			Y
4.1.2.1	Strategy Generation and Management	X			Y
4.1.2.2	IT Technology Planning	X			Y
4.1.2.3	Financial Management	X			Y
4.1.2.4	Service Portfolio Management Process	X			Y
4.1.2.5	Demand Management	X			Y
4.1.2.6	Business Relationship Management	X			Y
4.1.3	Service Design	X			Y
4.1.3.1	Solution Design Management	X			Y
4.1.3.2	Service Catalog Management	X			Y

VA-240920-NTT 02.1 Exhibit - Description of Services - Managed Public Cloud Services

4.1.3.3	Service Level Management	X			Y
4.1.3.4	Availability Management	X			Y
4.1.3.5	IT Service Continuity Management	X			Y
4.1.3.6	Capacity Management	X			Y
4.1.3.7	Security Management	X			Y
4.1.3.8	Risk Management (RSKM) Process	X			Y
4.1.3.9	Supplier Management	X			Y
4.1.4	Service Transition	X			Y
4.1.4.1	Change Management	X			Y
4.1.4.2	Change Evaluation	X			Y
4.1.1.5	PMO Risk and Issue Management	X			Y
4.1.4.3	Release and Deployment Management	X			Y
4.1.4.4	Service Asset and Configuration Management (SACM)	X			Y
4.1.4.5	Knowledge Management	X			Y
4.1.5	Service Operation	X			Y
4.1.5.1	Service Desk Function	X			Y
4.1.5.2	Incident Management	X			Y
4.1.5.3	Monitoring and Event Management	X			Y
4.1.5.4	Problem Management	X			Y
4.1.5.5	Service Request Management and Fulfillment Process	X			Y
4.1.5.6	Access Management	X			Y
4.1.5.7	Security Incident Management Process	X			Y
4.1.5.8	Request For Solution and Estimate	X			Y
4.1.6	Continual Improvement	X			Y
4.1.6.1	Service Review and Reporting	X			Y
4.1.6.2	Process Evaluation Currency	X			Y
4.1.6.3	Service Measurement	X			Y
4.1.6.4	Continual Improvement Plan Process	X			Y
4.1.6.5	Technical Innovation	X			Y
	QA Audit Plan	X			Y
5.0	Financial Management Processes				
5.1	Common Financial Management Processes				
5.1.1	Invoicing and Chargeback	X			Y
5.1.2	Disputes Process	X			Y
5.1.3	Financial Planning and Forecast	X			Y
5.1.5	Service Level Credits and Earnback	X			Y
5.1.6	Cost Savings Opportunity	X			Y
5.2+	STS XX ITFM RU Listing				
5.2.1	ITFM MSI RU Listing		X		
5.3	ITFM Mainframe RU Listing		X		
5.5	ITFM Managed Security RU Listing		X		
5.6	ITFM End User Services RU Listing		X		
5.7	ITFM Server Storage DC RU Listing		X		

VA-240920-NTT 02.1 Exhibit - Description of Services - Managed Public Cloud Services

5.8	ITFM Managed Print RU Listing			X		
5.10	ITFM VITA Internal RU Listing			X		
5.11	ITFM Data Network RU Listing			X		
5.12	ITFM Messaging-NTT RU Listing			X		
5.1X	ITFM MCS RU Listing				X	Y
6.0	Contract Management Processes					
6.1+	Common Contract Management Processes					
6.3	STS Contract Management (Peraton)			X		
6.5	STS MSS Contract Management			X		
6.6	STS SSDC Contract Management Information			X		
6.7	STS Xerox Contract Management Information			X		
6.8	STS EUC Contract Information			X		
6.9	STS Contract Management Information VRZN			X		
6.11	Messaging Services Contract Management			X		
6.1X	MCS Contract Management				X	Y
7.0	Relationship Management Processes					
7.1	Common Relationship Management Process					
7.1.1	Customer Satisfaction Surveys	X				Y
7.1.3	Third Party Vendors	X				Y
7.1.5	Complaint Handling Process	X				Y
8.0	Service Tower Supplier Operational Processes					
8.1	Common Service Tower Supplier Operational Processes					
8.1.3	Background Checks and Security Clearance Processes			X		
8.2+	Supplier Specific Processes					
8.2.2	Service Management Systems Support			X		
8.2.3	Security Clearance Tracking			X		
8.3.1.1	Mainframe Backup Process - Copy			X		
8.3.1.2	MF Job Request System Process			X		
8.3.1.3	Mainframe Access Request Process			X		
8.5.1.1	MSS Queue and Ticket Management			X		
8.5.1.2	MSS Security Response Plan			X		
8.5.1.3	MSS Security Monitoring Policy			X		
8.5.1.4	MSS Security Incident Response Process			X		
8.5.1.5	MSS Managed Security Services Comm Plan			X		
8.5.1.6	MSS Monitoring and Event Management			X		
8.5.2.1	MSS Managed IDS-IPS			X		
8.5.2.2	MSS Web Content Monitoring Process			X		
8.5.3.4	MSS Managed End-Point Security			X		
8.5.3.5	MSS Managed Firewall Service			X		
8.5.3.6	MSS Vulnerability and Compliance Management			X		
8.5.3.7	MSS Penetration Testing			X		
8.5.3.8	Data Security Process			X		
8.5.5.1	MSS Application and Source Code Security			X		

VA-240920-NTT 02.1 Exhibit - Description of Services - Managed Public Cloud Services

8.6.1	SSDC Server Provisioning		X		
8.6.2	SSDC Server Operations		X		
8.6.3	SSDC Storage Provisioning		X		
8.6.4	SSDC Storage Operations		X		
8.6.5	SSDC Database Provisioning		X		
8.6.6	SSDC Database Operations		X		
8.6.7	SSDC Enterprise Data Center LAN Provisioning		X		
8.6.8	SSDC Network Operations		X		
8.6.9	SSDC Enterprise Data Center and Facilities Management		X		
8.6.10	SSDC Backup and Recovery		X		
8.6.10	SSDC Backup and Recovery (GCP Review)		X		
8.6.11	SSDC Directory and Identity Management Services		X		
8.6.12	SSDC Asset Management AND Recovery		X		
8.6.13	SSDC Monitoring and Event Management		X		
8.6.14	SSDC Batch Management		X		
8.7.3.1	MPS Queue and Ticket Management		X		
8.7.3.2	MPS Desk Side Support		X		
8.7.3.3	MPS Asset Disposal Process		X		
8.7.3.4	MPS Consumables Management Process		X		
8.7.3.5	MPS Install Move Add Change Process		X		
8.8.1	EUC Queue and Ticket Management		X		
8.8.2	EUC Desk-Side Support Operations		X		
8.8.3	EUC Asset Recovery and Disposal		X		
8.8.4	EUC PC Refresh		X		
8.8.5	EUC Software Distribution		X		
8.8.6	EUC Warehouse-Depot Asset Management		X		
8.8.7	EUC Configuration Management Database (CMDB)		X		
8.8.8	EUC Agency-Specific Device		X		
8.8.9	EUC IMACs		X		
8.8.10	EUC Smart Hands		X		
8.8.11	EUC Request for Solution and Project Implementation		X		
8.9.21	VDN Engaging Verizon Subcontractors		X		
8.9.24	VDN Service Desk		X		
8.9.29	VDN Escalation Process		X		
8.9.38	NOC Operational Process		X		
8.9.56	VDN Configuration Management Database (CMDB) Processes		X		
8.9.57	VDN Queue and Ticket Management		X		
8.9.58	VDN Install and MACD (Moves, Adds, Change, De-installs)		X		
8.9.59	VDN Change Management		X		
8.9.60	VDN Request for Solution and Project Implementation		X		
8.9.62	VDN Event Management		X		
8.9.63	VDN Network Engineering		X		
8.9.64	VDN Security Management		X		

VA-240920-NTT 02.1 Exhibit - Description of Services - Managed Public Cloud Services

8.9.65	VDN Chronic Problem Management		X		
8.9.67	VDN Knowledge Management		X		
8.11.1	Messaging Queue and Ticket Management Process		X		
8.11.2	MSG Services Operations and Maintenance		X		
8.11.3	Software License Management		X		
8.11.4	MSG-NTT Data Lifecycle Management Plan		X		
8.1X.1+	MCS Supplier Specific Processes			X	Y
9.0	Customer Process and Documents				
9.1	Common Customer Processes				
9.1.2	Customer on-boarding		X		
	For SMM 9.1.2 - Supplier Service Requirements/Criteria			X	Y
9.1.3	Customer off-boarding		X		
	For SMM 9.1.3 - Supplier Service Requirements/Criteria			X	Y
10.0	Operational Reports - Reserved				
11.0	Communications				
11.1	Customer Communications Management	X			Y
OLAs	Operating Level Agreements				
	Atos - Iron Bow OLA		X		
	ATOS - Verizon OLA		X		
	Iron Bow - Verizon OLA		X		
	Iron Bow - Unisys OLA		X		
	Iron Bow - Xerox OLA		X		
	MSI - Atos (MSS) OLA		X		
	MSI - Peraton (MF) OLA		X		
	MSI - Unisys (SSDC) OLA		X		
	MSI - Xerox MP OLA		X		
	MSI - NTTDATA (MSG) OLA		X		
	MSI - Iron Bow EUC OLA		X		
	MSI - Verizon OLA		X		
	NTTDATA (MSG) - ATOS (MSS) OLA		X		
	NTTDATA (MSG) - IronBow OLA		X		
	NTTDATA (MSG) - MSI OLA		X		
	NTTDATA (MSG) - Unisys (SSDC) OLA		X		
	NTTDATA (MSG) - Verizon (VDN) OLA		X		
	Peraton - ATOS - OLA		X		
	Unisys - Peraton OLA		X		
	Unisys - Verizon OLA		X		
	Xerox - ATOS OLA		X		
	Xerox - Unisys OLA		X		
	Xerox - Verizon OLA		X		
	MCS - XXXXXX OLA(s)			X	Y