COMMONWEALTH OF VIRGINIA

VIRGINIA INFORMATION TECHNOLOGIES AGENCY (VITA)

SUPPLY CHAIN MANAGEMENT DIVISION

11751 MEADOWVILLE LANE
CHESTER, VIRGINIA 23836

REQUEST FOR INFORMATION (RFI) 2017-14

FOR:

SERVER, DATA CENTER, AND SECURITY SERVICES

Issue Date:	September 29, 2016
Due Date/Time:	October 21, 2016 @ 3:00 pm Eastern
Response Delivery Method:	E-mail attachment to Single Point of Contact
Single Point of Contact (SPOC):	Greg Scearce, VITA Supply Chain Management (SCM)
Telephone:	(804) 416-6166
E-mail Address:	gregory.scearce@vita.virginia.gov

NOTE: This public body does not discriminate against faith-based organizations in accordance with the Code of Virginia, §2.2-4343.1 or against a Supplier because of race, religion, color, sex, national origin, age, disability, or any other basis prohibited by state law relating to discrimination in employment.

VITA is committed to increasing procurement opportunities for small, women-owned, and minority-owned (SWaM) businesses, strengthening the Commonwealth's overall economic growth through the development of its IT suppliers.

TABLE OF CONTENTS

1. INTRODUCTION

The intent of this Request for Information (RFI) is solely to gather information; it is not a formal procurement. Responding to the RFI is not a pre-requisite to submitting a proposal for any subsequent procurement. Respondents should not provide any confidential or proprietary information.

Ownership of all data, materials, and documentation originated and prepared for VITA pursuant to the RFI shall rest exclusively with VITA. All information provided to VITA as part of this RFI will not be publicly disclosed, but shall be subject to public inspection in accordance with the §2.2-4342 of the *Virginia Public Procurement Act and the Virginia Freedom of Information Act.*

A. IT Infrastructure Services Program (ITISP) Overview

This procurement event is a component in VITA's overall strategy to implement a new IT Infrastructure Services Program (ITISP). This program will position VITA to fulfill its vision to "deliver agile technology services at the speed of business" by better balancing the needs of the individual agencies and the enterprise in a multisupplier ecosystem. The ITISP is intended to accomplish the following:

- **Maintain and improve service quality.**
    - Develop the capability to address evolving agency needs and create opportunities to improve service performance without degrading service reliability, security, and quality.
- **Ensure cost competitiveness – both now and in the future.**
    - Structure service offerings so they can be more easily compared to market services at market rates; offer a menu of service options to customers.
- **Create a platform view of service delivery that is highly visible and accountable.**
    - Provide for Enterprise and Agency visibility of consumption, cost, performance, and the responsiveness of suppliers. Establish a governance structure and forums to promote stakeholder engagement and improve the balance of agencies and enterprise needs.

Procurement of new services that will transition the Commonwealth from a single supplier model to an integrated multisupplier model is occurring over three waves. VITA has begun implementing Wave 1 of this transition by awarding a contract for Messaging services in July 2016 and a contract for IBM Mainframe services in September 2016. Wave 2 of this transition begins with this Request for Proposal ("RFP") soliciting proposals for the services of a multisourcing service integrator (MSI). That procurement was released on September 29, 2016 under RFP# 2017-03. The Wave 2 procurements are also intended to include services for Server, Storage, Data Center LAN, Data Center Facilities, and Managed Security Services (abbreviated as "Server, DC, and Security").

Respondents to this RFI are encouraged to review the publicly available RFP# 2017-03 documents for additional context. Note also that there will be a Pre-Proposal Web Conference for the MSI RFP, scheduled for Tuesday, October 4th at 2 pm. Information to register for the conference is indicated in the RFP Instructions for RFP# 2017-03.

B. RFI Purpose

VITA has decided to accelerate its MSI implementation, such that the contract for RFP# 2017-03 is awarded while the other Wave 2 procurements are still underway. The initial focus on the MSI RFP allows additional time at the front-end of the timeline to gather further market research for Server, DC, and Security via this RFI. This RFI will allow VITA to improve the quality of the resultant RFP or RFPs to be released around the end of 2016.

Currently, VITA's Wave 2 internal RFP teams are structured around two separate potential RFPs: 1.) Server, Storage and Data Center Services and 2.) Managed Security Services. However, VITA is interested in identifying the most efficient demarcation or bundling of these services between RFPs. For example, perhaps it would be more efficient to separate the Data Center facilities from the other Server services; or perhaps it would be better to include some or all of the Security services with the Server RFP. VITA anticipates resolving these decisions, and other questions as detailed in the Section 5 (Questions) below, in part by considering feedback obtained from marketplace participants via this RFI.

The Commonwealth has the following goals for the procurements:

Server, Storage, and Data Center Services

- Assume all existing Services for Server, Storage, Data Center LAN, and Centralized Data Center facility currently provided to the Commonwealth via the Comprehensive Infrastructure Agreement (CIA) with Northrop Grumman.
- Transition to the next generation of delivery for Server, Storage, and Data Center services to VITA and Customers, taking advantage of the ever-changing technology landscape while decreasing costs to VITA and Customers.
- Provide compute, storage, and Data Center LAN 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.

Managed Security Services

- Replace the existing security services included within the Comprehensive Infrastructure Agreement (CIA) with Northrop Grumman.
- Support VITA's Commonwealth Security and Risk Management (CSRM) directorate by acting as its operational "hands and feet":
    - Advising on risks and standards development
    - Assessing vulnerabilities and compliance (suppliers and agencies)
    - Provide security monitoring and integration tools across the environment
    - Respond to and address security risks and incidents
    - Provide tools and technologies to protect the environment from compromise
    - Provide security services that are adjustable to meet compliance needs of the Customer and adaptable to advancements in both security and technology industries
    - Establish, implement and maintain a secure enterprise information technology environment ensuring the confidentiality, integrity and availability of critical Commonwealth information and systems

- Provide VITA and its Customers with access to their data and metadata, in real-time

2. SUBMISSION LOGISTICS AND CONTACT INFORMATION

Issue Date:	September 29, 2016
Due Date / Time:	October 21, 2016 at 3:00 pm EST
Response Delivery Method:	E-mail attachment or CD sent to Single Point of Contact. Note: e-mail must be received by the due date and time; CD must be post-marked by the due date, but can be received later. E-mail attachments must be limited to 10 MB.
Single Point of Contact (SPOC):	Greg Scearce
Telephone:	(804) 416-6166
E-mail Address:	gregory.scearce@vita.virginia.gov
Mailing Address:	11751 Meadowville Lane, Chester, VA 23836
Pricing:	No pricing information should be submitted
Document Format:	Return this document, having populated Section 4 (Respondent Contact Information), Section 5 (Questions) below, and Section 6 (Feedback Regarding RFI Documents)
RFI Questions and Answers:	Suppliers may submit questions regarding this RFI at any time via e-mail to the SPOC.

3. OVERVIEW OF RFI DOCUMENTS

Within this RFI, VITA has chosen to release the following documents, which are drafts of some key documents anticipated for release in a final RFP or RFPs.

- Exhibit 2.1-a: Server, Storage, Data Center LAN Services
- Exhibit 2.1-b: Data Center Facilities Services
- Exhibit 2.1-c: Managed Security Services
- Exhibit 2.2: Cross-Functional Services
- Exhibit 3.1-a: Server, Storage, Data Center LAN, and Data Center Facilities SLA Matrix
- Exhibit 3.1-b: Managed Security SLA Matrix

- Exhibit 3.2-a: Server, Storage, Data Center LAN, and Data Center Facilities SLA Descriptions
- Exhibit 3.2-b: Managed Security SLA Descriptions
- Exhibit 4: Pricing and Financial Provisions
- Exhibit 4.1-a: Server, Storage, Data Center LAN, and Data Center Facilities Pricing and Volumes Matrix
- Exhibit 4.1-b: Managed Security Pricing and Volumes Matrix
- Exhibit 4.2-a: Server, Storage, Data Center LAN, and Data Center Facilities RU Definitions
- Exhibit 4.2-b: Managed Security RU Definitions
- Exhibit 4.4: Form of Invoice

4. RESPONDENT CONTACT INFORMATION

Please provide your contact information in the box below.

Contact Information	**Enter your response here, enlarging the box as needed**
Company Name	HP Enterprise Services, LLC
Company Mailing Address	13600 EDS Drive Herndon, VA 20171
Company Website Address	www.hpe.com
Name of Contact Person	Fred Duball
Contact Person E-mail Address	fred.duball@hpe.com
Contact Person Telephone #	(804) 212-9535

5. QUESTIONS

Please use the table to respond to the Commonwealth's questions.

Ref#	Category	Question	Supplier Response
A.	**Server/Storage Services**		
Q1.	Server/Storage	The Commonwealth has upwards of 10 non-centralized Data Centers in Agency-operated buildings, primarily in the metro Richmond area. What are examples of Suppliers' best practices in managing the Servers, Storage, Firewalls, and Data Center LANs in non-centralized (Agency) facilities?	HP Enterprise Services, LLC (HPES) bases its best practices in managing the Servers, Storage, Firewalls, and Data Center LANs on our years of experiences in resource staffing that delivers the skills to facilitate availability, reliability; and accuracy; technology selection and methods that deliver continuous optimization and efficiencies; and the adoption of industry guidance through well established and accepted standards such as Information Technology Infrastructure Library (ITIL) and ISO 9000 quality management systems standards. In our experience, most if not all assets can be consolidated into a centralized, fortified, resilient data center. Exceptions would be those applications that have to be located in the agency data center due to performance needs/sensitivity, those that cannot run across the WAN, or those that have other unique requirements that require locating in a local agency non-centralized data center. These exceptions challenge the opportunities to leverage the optimization and efficiencies of centralized infrastructure, toolsets, and staff. **HPES Best Practices Examples** • **Stabilize** by establishing the foundation that supports VITA's business goals and objectives. - Capture, understand, and document VITA's service management business objectives and technical requirements. Collaborate with VITA in validating the requirements to verify accuracy. - Establish a complete understanding of VITA's management policies, governance guidelines, security, and operational/ technical requirements. HPES

Ref#	Category	Question	Supplier Response
			accomplishes this through information exchange workshops, staff knowledge transfer, and documentation and exchange. - Staff the Server, Storage, and LAN services based on-site and remote access dedicated and leveraged staffing in support of managing centralized and non-centralized data centers. - Provide management services using the structure of the ITIL service model. • **Optimize** the environment. - Collaborate with VITA to overcome the challenges that exist in the current state. - Increase automation where possible, and eliminate disparate technologies and processes. - Streamline services and support across VITA Enterprise by optimizing staffing ratios; as an example, leverage a server or storage management cross-trained staffing model that relies on blended experience to deliver continual improvement of management solutions, configurations, response times, and flexibility. - Leverage on-site smart hands, subject matter experts, and remote access to manage and monitor infrastructure and data center workloads across VITA's enterprise data centers. - Engage and leverage HPE valued partners such as EMC, NetApp, Microsoft, VMware, and others to optimize technologies, best practices, configuration, and solutions. - Standardize toolsets across data centers by leveraging existing tools and recommending toolsets that would create extended value. - Implement and manage self-healing technologies to increase availability and improve efficiencies. • **Transform** the enterprise.

Ref#	Category	Question	Supplier Response
			- Work as a partner with VITA to assess the current state, jointly develop a transformation roadmaps, and work to transform Servers, Storage, Firewalls, and Data Center LAN management and infrastructure to a future state aligned with VITA's business objectives and goals. - Assist VITA in taking advantage of the New Style of IT with the objective of significantly reducing costs and enhancing service delivery and the end-user experience. As an example, HPES can assist in migrating your applications onto a cloud platform to increase agility and reduce costs. - Implement a single view of integrated technology and tools platform across the enterprise. - Implement HPES Availability Management capabilities for establishing the availability requirements of VITA's business; then plan, measure, and manage availability of the IT infrastructure to improve overall service delivery quality and consistency. By anticipating and minimizing failures, Availability Management can help identify, analyze, and reduce risks in line with VITA business needs. - Capacity Management – optimize capacity so it matches business objectives and requirements. Making sure the right capacity is always available can mean increasing capacity based on VITA business and IT needs or reducing or reallocating capacity so VITA pays only for the hardware, software, and support needed. - Work as a partner with VITA in consideration of the design and implementation of a centralized hybrid IT management platform that leverages a Service Broker approach. This approach would provide multiple levels of infrastructure that provide financially backed service level agreements (SLAs) in cloud environments. This means services can be configured with what is needed and also can be monitored and measured through the

Ref#	Category	Question	Supplier Response
			hybrid IT management portal. For on-premise solutions, Windows Server provides tiering, cache, and high performance remote direct memory access (RDMA) fabric so infrastructure can be defined to meet the performance needs of any service. In addition, it can be monitored and tracked with traditional tools and reported on through the Service Broker portal. HPE currently manages, operates, and monitors the following resources: • 82 data centers with 1.1M sq. ft. of raised floor space in 27 countries • 183 managed cloud environments • 6 global security operations centers 60 data recovery centers in 40 countries
Q2.	Server/Storage	What does the Supplier recommend for the length of the contract for Server, Storage, and Data Center Services? Please describe benefits and trade-offs.	Typical data center contracts are no less than 5 years and commonly 5 to 7 years. The reason is to minimize the cost, effort, and risk associated with migration of applications and data and all the related expenses. These migration costs are administrative in nature rather than directly fulfilling the end user's mission. This length of time also allows the service provider to institute standard processes and procedures that enable efficiencies to lower costs to the client. Shorter-term contracts are generally more expensive. Contracts longer than 7 to 10 years would not typically continue to see year-over-year reductions once the environment is fully stabilized. In addition, predicting data center costs beyond 7 to 10 years is not advisable, as, at that point, new technologies will have been introduced that the customer may want to adopt but are not included in the legacy contract.
Q3.	Data Center	What do you recommend for the length of the contract for the Data Center Facility for this type of environment?	We recommend a shared facility, as a dedicated facility requires a substantial fixed cost investment where the return on investment could stretch into 10 to 15 years. Using a facility that supports multiple clients allows the contract term to become

<table>
<tr><th>Ref#</th><th>Category</th><th>Question</th><th>Supplier Response</th></tr>
<tr><td></td><td></td><td></td><td>less important because the fixed investment is shared among multiple clients with varying contract terms, thus reducing the risk to the service provider and reducing the cost to the client.</td></tr>
<tr><td>Q4.</td><td>Server/Storage</td><td>What does the Supplier recommend for technology refresh rate for the different types of Devices in VITA's environment? Is there an impact on the length of the services contract?</td><td>The traditional technology refresh rate is on a 3- to 5-year cycle. In terms of today's rapidly evolving and changing technology, age is not the only determining factor. Other considerations include the following:
Adoption of technologies like server virtualization make it increasingly difficult to stick with traditional hardware refresh rates.
Increased business requests and requirements (more computing)
Demands for more service speed and efficiency
Shifting workloads and application requirements
Business plans, goals, and means to meet IT requirements.
<table><tr><th>Device Type</th><th>Refresh Rate</th></tr><tr><td>Server</td><td>3 years, depending on server</td></tr><tr><td>NAS SAN Storage Arrays: SSD, FC, SAS</td><td>5 years</td></tr><tr><td>Tape Systems: Library/Tape Drives</td><td>5 to 7 years</td></tr></table>Service contracts typically align with refresh every 3 to 5 years. The impact of a service contract occurs with the end of product life and end of service. Extending services beyond this time introduces risk due to parts availability and compatibility with modern applications.</td></tr>
<tr><td>Q5.</td><td>Server/Storage</td><td>The Commonwealth is interested in a separate hardware charge in the Server RUs to account for the initial capital outlay for physical servers. Is there a better way to represent the cost differences and hardware refresh cycle</td><td>We recommend including separate hardware Resource Units (RUs), as the current RU structure does not differentiate between the sizes of the computing requirement. We have</td></tr>
</table>

<table>
<tr><th>Ref#</th><th>Category</th><th>Question</th><th>Supplier Response</th></tr>
<tr><td></td><td></td><td>in the Server RU structure?</td><td>proposed a model for hardware, software, and services in our answer to Question 7 below. In addition, cloud services options provide the opportunity to avoid capital outlays entirely. Cloud offerings can be structured as both private and public clouds and offer the ability to purchase infrastructure capacity on a pay-per-use basis. Having multiple options provides greater flexibility in ordering only required services.</td></tr>
<tr><td>Q6.</td><td>Server/Storage</td><td>The Commonwealth is proposing tiering of services for Server and Storage in an attempt to align costs with availability and performance. Based on your experience, do these tiers of service have any challenges in developing a solution? Do you have experience with these service tiering model? Do you have any recommendations or enhancements for the Commonwealth to consider?</td><td>Based on your experience, do these tiers of service have any challenges in developing a solution?
HPES brings the experience to develop the service tier models with a focus on cost alignment.
The biggest challenge in developing the tiered solution is factoring in costs associated with the highest level of tiers and matching applications to the correct tier. HPES would work with the Commonwealth to identify and recommend based on business impact the correct level of service for an application. We often find that if we present application owners with a menu without adequate guidance, they will want the highest level of support; this might not match the business objectives. By matching the two, we eliminate unnecessary high costs of Operations and Sustainment. Although the tiers required are dependent on the specific needs, we include for your review the most common industry standards we see.

Typical Industry Standard Tiers Support Levels
<table>
<tr><td>Average Server Availability – Gold</td><td>99.900%</td><td>Critical Application, Major Impact to the Commonwealth</td></tr>
<tr><td>Average Server Availability – Silver</td><td>99.500%</td><td>Internal Business Support Application or Minimal Impact to the Commonwealth</td></tr>
</table></td></tr>
</table>

Ref#	Category	Question	Supplier Response

Average Server Availability – Bronze	99.000%	Development/Test environments

HPES' experience in the development and deployment of tiering of storage services is at the core of our solution capabilities. The solutions and their cost to support and deliver these service capabilities are highly dependent on the flexibility of storage technology selection, the geographical locations, and the service level parameter requirements that determine the service level performance, availability, recovery time objective (RTO), and recovery point objective (RPO). HPES has seen challenges in keeping costs reasonable when solutioning the Platinum and Gold tiers of services. This is mainly due to the complexity of the solutions that enable the availability and performance required to meet these service levels. Areas for consideration that can have a positive impact on the solution complexity and cost are the RTO and RPO requirements—seconds and minute response and availability solutions are going to be more complex and costly than hourly response and availability solutions. HPES also advises our clients to keep the number of application and volumes of data in these tiers to a minimum. Consider use of throttling techniques that prioritize workflows and assist with managing latencies. Consider geographical distance between data centers.

Storage Availability

Archive Storage NAS	Midrange Storage NAS
99.9% with multi-NIC connectivity	Base NAS: 99.9% Enhanced NAS: 99.99% Both require multi-NIC connectivity

Ref#	Category	Question	Supplier Response

Midrange Storage SAN	Enterprise Storage SAN
99.99% when multi-pathing is provided	99.999% when multi-pathing is provided

Do you have experience with these service tiering models?

HPES has 50+ years of experience developing solutions and managing complex global IT environments. While operating within the ITIL-based framework, we would leverage this experience in developing the service tiering models with a focus on performance and availability cost alignment.

Do you have any recommendations or enhancements for the Commonwealth to consider?

HPES' recommendation is to leverage both traditional data center and cloud solutions. This flexibility will enable architects and designers to solution availability and performance capabilities that align with optimal costs. Enhancements to consider are as follows:

- Workload optimization – finding the right platform for each application using predetermined criteria co-developed by VITA and HPES. Once the criteria are defined, VITA can select or build hosting platforms that satisfy the criteria including traditional, private cloud, and public cloud. Applying the right platform for each application makes sure that the application receives the appropriate level of support in the most cost-effective environment.
- Converged Data Protection – this emerging technology integrates and leverages both primary storage and data protection storage technologies to improve data protection, reduce recovery time, and simplify overall management.

Ref#	Category	Question	Supplier Response
			• Continuous Data Protection (CDP) technologies for tier 1 and 2 – CDP provides disk based continuous data protection with additional recovery points. Federated deduplication and catalyst technologies that enhance performance by deduplicating anywhere—at the application source, at the backup server, or at the target—taking full advantage of high and low bandwidth where possible with capabilities that span the enterprise with the option of having the same data protected at multiple sites.
Q7.	Server/Storage	The Commonwealth currently spreads costs across a very simple RU model. Do you have an enhanced RU model that could offer a larger variety of services while minimizing the RUs and their complexity?	There are many options for providing an RU structure. Although a very simplified structure might be preferred, you do not see the full benefits of all the new technologies available. As you have already identified two of the key elements in your RU structure—operating system (OS) type and service level—there are other factors to consider. HPES recommends a broker of services that offers a single

Ref#	Category	Question	Supplier Response
			consolidated catalog including RUs from traditional, private cloud, and public cloud. This would increase the number of choices for the Commonwealth customers, simplifying the process of finding the appropriate service and exposing the associated costs to your customers when making those choices; this will encourage the rapid adoption of new services. Once the customer selects the required services, the broker provides rapid provisioning and can be used to scale for an elastic and flexible environment. Reporting is simplified on the services being provided and costs associated with them. HPES would integrate the service broker and catalog of services as they relate to our tower with the multi-supplier integration (MSI). In addition to the type of environment and the financial benefits of one environment over another, other optional services are also integrated into the service catalog. This prevents over inflation of costs for services that are not required in every instance. You are billed for only the number of instances you consume—and, again, the costs are exposed so that the business and financial decisions are made together. Some examples of what the catalog might offer are as follows: • Cloud T-shirt sizing for vCPU, vRAM, Storage • Physical servers that have a base option and add-on components for Memory and CPU type, which can have multiple core sizes • Tiered service levels: Platinum, Gold, Silver, Bronze • SQL or Oracle System DBA and Application DBA • Tiered Storage • Directory Services Web and Application Services
Q8.	Server/Storage	The Commonwealth is including Bronze thru Platinum service levels for Server as examples of service categories. What would be required to implement this model in the	Based on VITA-RFI 2017-14 - 02.1-a Exh (Description of Services - Server-Storage-Data Center LAN), a Commonwealth potential model could be as follows:

Ref#	Category	Question	Supplier Response
		Commonwealth?	• **Platinum** (e.g., Very High Availability, Multi-site Active/Active, Multi-site Clustering, Geographically Dispersed, Hot/Hot Sites) • **Gold** (e.g., High Availability, Multi-site Active/Passive, Geographically Dispersed, Failover, Hot/Warm Sites) • **Silver** (e.g., High Availability, Single Site Clustered Services, Not dependent on a single server point of failure, cluster in VITA, or VITA Customer Data Center) • **Bronze** (e.g., Single Server, Mirrored OS, Server in VITA, or VITA Customer Data Center) To implement models that would include Bronze to Platinum options, HPES would work closely with VITA and the agencies to assess the application layer to determine which business function requires which service level profile. From there, the services would be architected to accommodate the levels of service required. As an example, for Platinum support not only do you need the redundant architecture and failover software, but most maintenance agreements will only support a 4-hour response time—not 2 hours. To meet this SLA, HPES would recommend that the Commonwealth have spare equipment on hand in the data center. Another important aspect of the service levels is the support required from a full time equivalent (FTE) effort. HPES would build the team based on required effort to manage to these different levels. As we work with VITA and the agencies to review the current architecture, we will identify gaps that might prevent the systems from meeting the service levels as well as identify systems that might be classified at a higher level than is necessary and reduce costs. As we recommended in Question 7, having a catalog of service will provide an on-going means to present these tiered service categories and provide transparency to VITA agencies and users on costs associated with each tiered service level.

Ref#	Category	Question	Supplier Response
Q9.	Server/Storage	Do you see a better way to bundle or spilt the services we are requesting, in order to more effectively integrate with other towers (including MSI), and obtain more flexibility in the Commonwealth's IT environment while maintaining appropriate Governance and security?	A Hybrid IT Management Service Broker platform, as described in Question 7, with a consolidated service catalog would provide a robust set of services that can be bundled or used individually to meet the needs of the environment or individual deployment. Integration across multiple cloud platforms, and even traditional environments, through this model provides even more flexibility in deployment options and service catalog options—all while maintaining common security and governance standards.
Q10.	Server/Storage	Are their new Storage offerings, like Object Based Storage or predictive storage, that the Commonwealth should include in storage or enhanced services? How do you offer and charge for virtual storage?	HPES recommends review and consideration for the following trending technologies: Solid-state arrays (SSAs) solution opportunities include deployment for performance in databases and consolidation in highly virtualized environments such as virtualized server infrastructure and hosted virtual desktop infrastructure. Market adoption has matured, cost is becoming competitive with high performance hard disk drives (HDD), and capacities have increased. HPES is the first storage vendor to offer the 7.68 and 15.36 TB SSDs. Software-defined storage (SDS) enables you to create a pool of shared storage on industry-standard servers, without the need for dedicated arrays. HPE StoreVirtual technology runs within VMware vCenter, Microsoft Hyper-V, or Linux KVM environments on the same server as your virtualized applications. It creates a scale-out iSCSI SAN that provides capacity and advanced data services, such as tiering, or clustering for any physical or virtual server. Converged Data Protection is an emerging technology that closely integrates primary storage and data protection storage technologies. HPE Recovery Manager Central (RMC) employs a direct backup model to orchestrate the snapshot lifecycle and protect the data on a separate backup target without a backup application. With RMC backup, once the first full backup is complete, each subsequent backup is a differential, making it

Ref#	Category	Question	Supplier Response
			significantly faster than traditional backup methods—particularly for higher volumes of data.
Q11.	Server/Storage	The Commonwealth is interested in ensuring it provides optimal storage performance and availability for VITA and VITA's Customers. How do you propose to provide and measure this performance?	In collaboration with the Commonwealth, HPES recommends leveraging VITA's existing service operations, designs, and existing technology and tools where appropriate for the initial measurement of performance and availability of performance reports and data to establish what type of performance and availability VITA and VITA's customers are currently experiencing. HPES would then engage in a discovery phase for data capture and analysis to determine available measurements of performance capabilities and identify which systems and storage solutions are and are not meeting existing service levels. We would then work with the Commonwealth to establish the service levels needed to provide the optimal storage service and availability VITA and its customers desire and expect. With the agreed SLAs in place, HPES would implement Availability Management plans and program designed to manage availability of the IT infrastructure to improve overall service delivery quality and consistency. This is accomplished by anticipating and minimizing failures and identifying, analyzing, and reducing risks in line with your business needs. At its core, Availability Management plans for the expected and prevents business disruptions by employing both reactive and proactive activities. We report and analyze the availability statistics, assess the impact of changes in the IT environment, recommend improvements, and collaborate with you to manage IT steady state and growth. A key output from Availability Management is the identification of issues requiring Problem Management before they develop into a business disruption event. This is accomplished by establishing the components within the infrastructure to be managed and reported. Reporting is based on metric collection and component levels providing measurements that communicate component availability that

Ref#	Category	Question	Supplier Response
			integrates, consolidates, and converts performance and usage data leveraged from the applicable underlying service. These reports incorporate user-defined parameters—such as expected uptime and exception hours—to provide details, including a historical view, on component availability. Additionally, components are grouped together to provide alternate views, such as Regional, Service, System, and so forth. HPES would forward availability reports to those recipients VITA designates on a monthly or agreed schedule. As a next step, we would implement Availability Planning. This assists in understanding the impact availability has on VITA's business, and provides recommendations to make certain that ongoing service availability matches your future needs. By examining and evaluating performance data from the current environment, Availability Planning can determine whether your current needs are satisfied and what levels you will need for the future. By examining and evaluating performance data from the current environment, Availability Planning can determine whether your current needs are satisfied and what levels you will need for the future. Using output from Availability Reporting, Availability Analysis and Optimization builds on those reporting activities to focus on management of availability-related issues and risks. Your HPES Service Delivery team regularly reviews the data in the availability reports, along with other IT Service Management data such as Service Level Measures and Problem Management Data (if available), to identify opportunities for improvement. We conduct additional analysis on the systems or components where the level of service availability does not match the business needs or where the service availability has an unfavorable trend. HPES then provides recommendations to optimize the availability, based on the results. Benefits of HPES Availability Management include the following: • Quantifies IT service risk so it is easily compared against

Ref#	Category	Question	Supplier Response
			business benefits • Defines a cost-effective and acceptable level of service, which prevents over-delivery and unnecessary maintenance costs on resilience building • Provides visibility of IT performance in a business context, enabling effective management decisions to be made • Prevents business disruptions by matching IT resources to rapidly changing business requirements • Reduces the number of incidents related to availability issues along with the subsequent cost of downtime To provide ongoing optimization, HPES would engage with valued HPE partners such as EMC and NetApp and others to develop and provide to the Commonwealth the system and storage solution recommendations that will deliver the continued optimum storage and availability VITA and its customers expect and require. This provides a holistic view to service delivery as it relates to Server, Storage, and LAN within a solution design with future design plans for enabling all metrics collections to be integrated within the Commonwealth's planned MSI.
Q12.	Server/Storage	The Commonwealth has traditional x86 virtual servers, but it is also interested in the capabilities of a private cloud. Could they be combined or left separate? Please describe how this could be accomplished most effectively.	Each type of workload needs to be deployed on the best platform for its unique characteristics, considering cost, performance, security, regulatory, compliance, and other criteria. Not all applications and workload are appropriate for cloud platforms; a traditional virtual server hosting option will remain the best choice for some applications. HPES recommends that the two environments be integrated through a hybrid IT management platform or service broker. **Service Broker Platform** – The service broker should provide governance over a collection of varied IT and cloud service providers, control "shadow IT," and establish service efficiencies by giving a single view of enterprise IT spending, service

Ref#	Category	Question	Supplier Response
			provisioning, internal usage patterns, and unified governance. **Hybrid IT Management Platform** – The broker platform should use a high level of automation and orchestration to integrate and manage across hybrid clouds and the traditional data center, but also interact with manual or semi-automated services and processes.
Q13.	Server/Storage	How does Database as a Service make sense for an Enterprise like the Commonwealth? Do you have any recommendations for how to charge for enhanced Database services (i.e., Development DBA)?	While the adoption of Database as a Service (DBaaS) requires a level of standardization across the enterprise, it can offer the Commonwealth a number of benefits. These include quicker deployments, enhanced organizational efficiency, elastic consumption of services, and lower operational costs. While DBaaS services include the cost of a system database administrator (DBA), the cost of other DBA services (development, application, and so forth) are typically purchased on a time-and-materials basis.
Q14.	Server/Storage	The Commonwealth wants to provide cost effective solutions to VITA and the Agencies. What do you describe as the key cost and value drivers that would help the Commonwealth offer services that are not cost prohibitive to deliver? Do you see any requirements in the description of services in this RFI that would cost more to meet than the business value they provide?	Within VITA-RFI 2017-14 - 02.1-a Exh (Description of Services - Server-Storage-Data Center LAN), many requirements are specified that can be provided in a cost-effective manner to VITA and its agencies. However, we would need to create the proper RUs to cost so that base services are not inflated. HPES recommends that services start with the base unit such as services for OS server management by type of OS: Physical, Virtual, Host, or Cloud. Then the additional services such as DB, Web Application Hosting, AD, Batch Management and Scheduling, Middleware, etc., are chosen as required and layered on top of the base services. VITA and its agencies can pick from this menu of services only those services required. As servers and functions change over time, those services can be adjusted, providing the most flexible environment at a reasonable cost. HPES recommends a Service Broker solution to provide an organized process and the financial controls needed to request services to meet VITA business requirements. We use people, processes, and tools to automate the flow of information

Ref#	Category	Question	Supplier Response
			between service requestors and operational teams, providing process management from request receipt through payment. The workflow address two types of service requests: • Standard service requests (SSRs): Requests for products and services that have pre-agreed prices and consistent delivery steps and that comply with classification business rules (mix and quantity thresholds) • Non-standard service requests (NSSRs): Project-related requests for add-on services or products within the current master service agreement and not listed in the standard services catalog This solution would allow agencies/consumers to select the most cost-effective service based on agency/consumer input using the service request workflow. This approach provides the most cost-effective and transparent solution that continually delivers the best value to VITA and its clients.
Q15.	Security	The Commonwealth is interested in an Enterprise Key Management System for compliance and security. How do you propose the Commonwealth request Key Management services?	Key Management Systems (KMS), including the HPE KMS, are just a few examples of installed appliance-based service modules that support effective key management and compliant key protection practices across the enterprise. **New Baseline for Compliant, Secure Key Management** Currently compliance for Key Management has taken a larger place in the list of areas for enhanced controls and investment by state and local governments. This is largely due to the need to increase controls on and use of varied key management processes that form the core of securing all user-to-machine, user-to-user, and machine-to-machine interactions across server and storage environments. In combination with identity and access management expertise, HPES is knowledgeable of the full range of options provided across industry and will work with VITA to establish a best “fit for purpose” approach for selection and acquisition of KMS. **Selections and Recommendation Founded in Both Technical**

Ref#	Category	Question	Supplier Response
			and Operational Expertise As both a support and sustainment partner to client-owned and -operated infrastructure and an infrastructure provider ourselves, HPES brings a unique user perspective to Key Management. Within the server and storage environment, the use of KMS components is a standard best practice that HPES will continue to employ effectively in delivery of the VITA solution sets. HPES will evaluate and view a full range of modalities and configuration-based applications for Key Management, including Software as a Service (SaaS) and integrated closed or site-based platforms, using requirements evaluated by a combination of VITA security teams and our HPES Enterprise Key Management Application and Solutions specialists. These professionals use a full range of vendor applications, devices, and service provisioning options to compare the operational and security compliance requirements for managing keys and perform comparative analyses to determine appropriate, cost-effective options for the VITA team. **Short List of Summaries and Subfactors for Consideration** VITA receives these summary and options immediately from the team upon a review of the VITA standards and storage and server architecture and provisioning processes and workflows. As a result, the Key Management platform options can be narrowed down based on the following factors: 1. Regulatory Requirements or Standards 2. Operational Control KPIs 3. Numbers and Complexity of Key Management Requirements 4. Matrixed Commercial Off-the-Shelf (COTS) and Commercial Service Offerings Consistent with the VITA Requirements. **Solid Use Case Basis for the Resulting Options and Recommendations for KMS Acquisition and Implementation**

Ref#	Category	Question	Supplier Response
			Based on this rapidly assessed and validated level of detail, we would then provide the options best suited to the specific VITA operational and technical environments, alongside a solid process and concept of operations understanding and risk assessment to key assignment, KMS access restrictions and automation, process simplification, standards enablement and established best practice KMS selection, and ongoing management sustainment. Again, the overall use cases would inform these options with cost and other factors appropriate to provide guidance to VITA on the selection and use of KMS toolsets to their maximum effectiveness over the program lifecycle. Our fully vendor independent recommendation would focus solely on best value to the VITA user and stakeholder community. By using this open process for requesting Key Management Services, the VITA team will be well served by the managed and multi-vendor/supplier and services approach leveraged across multiple similar Multi Supplier Integration (MSI) successes HPES has created for state and local governments. Once the process for evaluation is established, VITA will make its decisions based on the unbiased and open information provided by the team and will leverage the overall processes in place for both procurement and support requests related to Key Management Systems.
Q16.	MSI	Identity and Access Management (IAM) services and the systems supporting those functions are currently split between multiple providers. How do you propose bringing these services together to provide a single integrated service?	**Working within a Multi Supplier Environment for Identity and Access Management (IAM)** HPES provides a unique perspective for the integration of all enterprise systems and platform providers to be integrated into a multi-supplier/vendor integration (MSI) community for identity and access management. This best practice would be used as the standard opening template for the VITA program. **Understanding of IAM Platforms at the Core of Design and Deployment, with Best-in-Class Experience Across Multiple**

Ref#	Category	Question	Supplier Response
			Vendor Platforms and Global Scale Implementations IAM comprises identity components, access components, and repositories. Industry best practices for IAM recommend a single centralized integrated framework. In our experience, there are multiple ways to create a roadmap for system unification and standardization when faced with legacy multi-platform configurations, capabilities, and interoperability challenges HPES will look toward a solid roadmap of options and immediate steps to unify and standardize. These will include a centralized user provisioning/lifecycle, authentication and authorization that can be effectively managed through integration toolsets already available and other COTS-based integrated audit and control functions for unified data entry, duplication elimination and credential and key management that can sit behind the platforms as new standards replace end of life, and technical refresh-ready components. In this way, we maintain and extend the lifespan of the backbones of an IAM framework, allowing VITA to integrate with multiple providers for the long term while looking toward economies of scale and standardization moving forward. Through establishing a central single integrated IAM framework, VITA can improve its security posture as well as benefit from improved compliance, reduced risk, improved operational efficiencies, and ultimately technology enabled IAM-compliant business agility. Moreover VITA can eliminate costs associated with design and development "one-offs" in each application development group; reduce or eliminate platform-specific hardware and software that supports security administration activities; and ease application integration by providing a common authentication and authorization infrastructure. **Immediate Possibilities for Successful Vendor Integration in an MSI Environment**

Ref#	Category	Question	Supplier Response
			To achieve transition success from multiple providers to a single integrated system, HPES recommends VITA follow system development life cycle (SDLC) principles with an Agile approach for implementation. This includes executive and business buy-in, identifying your drivers (security, cost, risk, compliance, operational, agility), and a strong project management methodology. Using a phased deployment—and not rushing to implementation—is critical in integrating with multiple providers. **Building a Coherent and Actionable IAM Roadmap** VITA can begin with its processes, in collaboration with HPES, to perform discovery through analysis of current provider processes, documentation, or interviews. Our approach is to document the number of systems and applications affected and determine whether they are established or in-flight. VITA will be presented a careful and detailed overview of the transition migration process and plan to the single centralized system stakeholders. Multiple providers' application integrations will be prioritized based on input from the VITA team. VITA's resulting application integration process will include performing a technical application status review for Authentication and/or Provisioning/Access Management using proven best practices and specific lessons learned from successful integration of IAM platforms from across HPES and HPES user communities and clients. VITA will then be able to leverage common identity toolsets that can connect to both the new single system and disparate systems to capture information or synchronize data for relying parties, identity providers, schemas, any custom coding, access rights, and user data in the disparate systems and port this information to the centralized IAM system. Understanding the importance of these key items will help define how VITA's deployment will be staged and scheduled,

Ref#	Category	Question	Supplier Response
			with appropriate levels of functionality and room for growth that mirrors VITA's budgetary and user community as well as security milestones. **Ultimate IAM Benefits, including Cost and Operational Efficiencies, Can Be Realized in a HPES Facilitated Unified Platform** Once VITA has chosen and implemented a single centralized IAM framework, the enterprise will see the benefits of the system outside the information security domain as well. Non-IT resources—such as physical security access devices and mobile (and other devices)—can be better managed at the time of issuance. When the system or the user of the device leaves the enterprise, access is revoked. This results in full visibility, rapid response, and full compliance of the IAM solution set across the VITA server and storage architecture environment, with potential for ongoing efficiencies of scale and ultimately unified production and management environments that support ongoing investment returns and benefits to the VITA effort.
Q17.	MSI	The Commonwealth has defined the cross-functional requirements in Exhibit 2.2. Do you have any comments in the structure and handoffs identified in this document? Do you have any prior experience working with MSIs? Do you have any recommendations regarding the approach for how the MSI should interact with the other suppliers?	**Do you have any comments in the structure and handoffs identified in this document?** • Throughout VITA-RFI 2017-14 - 02.2 Exh (Description of Services - Cross Functional), it mentions "will participate." Clarifying the expectations of "participate" would be helpful. The RFP should define the frequency of these activities and also what deliverables the provider should have produced to assist/participate in each of the ITIL activities. • It would be beneficial to note whether activities outlined in the document are firm fixed price *or* are to be priced by a rate card or time and materials (T&M). • We find helpful having RFPs specify that each respondent discuss their experience and differentiators for ITIL / MSI

Ref#	Category	Question	Supplier Response
			experience. Since ITIL is an industry standard, having providers stress their experience and differentiators provides a much more valuable selection criterion. • VITA-RFI 2017-14 - 02.2 Exh (Description of Services - Cross Functional) has a significant amount of detail on expectations outlined. We have found that summarizing expectations and looking for experience and differentiators have more value in the selections process. ***Do you have any prior experience working with MSIs?*** We have deep expertise in multi-supplier and hybrid environments, managing primary technology (network, applications, data center, end user), outsourcing partners, plus secondary service providers—management of full delivery model. HPES delivers MSI services to many of our top 200 enterprise accounts. We engaged with more than 30 of our top 200 enterprise accounts, managing an average of six primary outsourcing partners and 20+ secondary service providers. Our MSI ITIL-based Service Reference Architecture platform supports more than 11K daily users. ***Do you have any recommendations regarding the approach for how the MSI should interact with the other suppliers?*** The MSI must coordinate all aspects of your vendor relationships, supporting your IT as a heterogeneous environment that integrates people, processes, and technology into a single enterprise solution. This not only mitigates the complexities of multi-sourcing IT service management, an MSI must align the entire IT organization to the same objectives, business goals, and operating rules. Fully implemented, MSI provides the quality and control to measure performance against established service levels and key performance indicators while making certain that the entire environment is working at peak performance. An MSI must have mature processes and procedures to assist suppliers in providing the following:

Ref#	Category	Question	Supplier Response
			• High-quality service delivery through best practices, industry-leading tools, and alignment to established global standards such as ITIL and Six Sigma • Robust and reliable end-to-end performance data to support your business decisions • Reduced risk of human error by automating and standardizing processes • Improved speed and responsiveness to introduce new suppliers • Replaces your fluctuating capital expense with a predictable operational expense, allowing to better manage IT budgets and freeing funds for business innovations • Enhances capacity planning, enterprise architecture, and long-range planning of the entire IT landscape • Creates transparency of IT operations and predictable IT services The MSI must include both a governance service framework and a core set of defined integrator packages and flexible features that can be added or tailored based on specific needs and requirements. This enables full—but always flexible—management of all your IT services. The MSI must take care of every aspect, including the following: • **Governance** – aligns IT policy, service providers, and internal decision makers to create a single, highly functioning organization - Committee Structure - Business Architecture - Communication and Escalation - Risk Management - Compliance Management - Continual Service Improvement - Supplier Management

Ref#	Category	Question	Supplier Response
			- Contract Administration and Dispute Management • **Service Operations** – coordinates problem resolution and change across the various technical towers and service providers - Incident Monitoring and Reporting - High Priority Business Situation Execution - Problem Monitoring and Cross-Tower Coordination - Change Monitoring and Cross-Tower Coordination - Release Monitoring and Reporting - Basic Configuration Aggregation • **Business Operations** – manages suppliers, contracts, and financial arrangements to make certain IT is financially sound - Standard and nonstandard service request management - Financial management, including Invoice Aggregation, Presentment, and Forecasting • **Service Planning and Design** – makes sure that IT changes and evolves in support of the business, not just for the sake of technology - Catalog Content Coordination - Service Level Performance Monitoring - Capacity Aggregation and Reporting - Availability Aggregation and Reporting • **Service Build and Transition** – monitors and enhances how evolving technology brought into the IT environment is consumed • **End-User Services** – delivers multiservice and vendor service desk, online support, and the service catalog the way the end user wants to consume them - Web-based Executive Portal - Management Reporting

Ref#	Category	Question	Supplier Response
			- Secure Client Access and Role-based Reporting The MSI must understand that a customizable solution embracing both internal and external service providers for your IT environment addresses both business and financial objectives. A "one-size-fits-all" solution with rigid and inflexible services fails to deliver true value in a multi-sourced configuration. The MSI solution provides the governance, processes, procedures, and skilled IT professionals needed to monitor and measure your outsourced services. MSI foundation services should be designed to significantly improve and streamline the management of multiple suppliers: • **Service Governance** – aligns IT policy, service providers, and internal decision makers to create a single, highly functioning organization • **Service Integration and Management** – assures delivery of services aligned with established service levels required for a stable IT environment • **Service Planning and Design** – collects, analyzes, and aggregates service provider generated service level reports and reviews performance to SLAs • **End User Services** – Global Service Desk – Provides a Global Service Desk and a single point of contact for end-user requests. While not included in the foundational services, HPES can provide the necessary functionality if it is not in place today. • **Business Integration and Management** – Engages a service provider(s) to define services, catalog items, delivery sequencing, and catalog aggregation if necessary; review content; and establish ongoing governance. • **MSI End User Services** - Global Service Desk – Provides a single point of contact (SPOC) for end-user services and requests o Providing Extended Case Management

Ref#	Category	Question	Supplier Response
			o Performing first call resolution o Recording and escalating Priority 1 and 2 incidents for resolution when necessary o Facilitating the assignment of Priority 3 and 4 incidents to the owning service provider with proper follow-up and closure o Receiving and dispatching standard catalog-based service requests to service provider o Monitoring and management of all classes of tickets, regardless of service provider or resolver group - Business Integration and Management – Defines IT Service Catalog items, engages and service provider(s) to define services and delivery sequencing, aggregates provider services and catalogs, holds content review before publishing, and establishes the ongoing governance for review of changes • **Service Integration and Management** - Service Operations and Integration Management Services - Critical incident management - Service Request Management Processing Standard Requests: o Receiving a user's request for IT product(s) or service(s) for services listed in the Services Catalog o Approving the request o Issuing the request to Service Integration o Verifying the request by Service Integration o Issuing the request for service to the service provider(s) o Delivering the service by the service providers(s) o Closing the request - Processing Variations to Standard Requests: o Processing Agreed Variations to Standard Requests – including request for provision and collation of

Ref#	Category	Question	Supplier Response
			proposals and delivery of variations to service. o Processing Ad Hoc Requests for Services and Products – Supporting requests for ad hoc services, provision of proposals, and the delivery of service(s) o Reject and Cancel a Request – Manage a service provider's rejection of a request for services because it does not meet required and agreed criteria, or where cancels a request for service prior to fulfillment Catalog Change Management – Manage changes to the Services Catalog by Service Integration and service providers
Q18.	MSI	Do you see any benefits or challenges in requiring the Data Center facility provider to also be responsible for providing common operating monitoring groups in the same solution (e.g., CMOC, ITOC, SOC, NOC)?	HPES sees great benefits in having the Data Center facility provider be responsible for providing the common operating monitoring groups. This holistic approach to enterprise management provides the ability to see the dependencies between the CMOC, ITOC, SOC and NOC. An example would be a Denial of Service attack that directly impacts performance. If those systems are independent, the issues seen independently might take longer to identify and resolve. It would take more time to have each of the monitoring agent representatives pulled together through the MSI and more resources required to identify and resolve the problem. By having the systems under the data center facility provider the systems can share data and the correlations between what is happening can be made quickly to reduce the time to identify and ultimately time to restore, which reduces risk to the Commonwealth. In addition, this approach offers end-to-end efficiency in setting thresholds, reporting, notification and escalation, and performance and capacity monitoring and management requirements. Many of these tasks if independently managed will need to be collected back together to truly understand how the environment is working as a whole and who will be impacted by specific changes or issues. Therefore, HPES

Ref#	Category	Question	Supplier Response
			recommends a centralized monitoring and management approach as the most optimal and efficient solution. The MSI and data center provider will be able to work together to quickly resolve issues that cross boundaries and coordinate more effectively with each provider. We also recommend the use of integrated monitoring and management for the IT infrastructure and the data center facilities infrastructure to achieve efficiencies in operation, asset management, capacity management, and energy management. We will collaborate with the MSI to make sure that the tools selected integrate with MSI-provided tools, allowing access to provide transparency in how the data centers are supported and managed. **Data Center Management Tools** HPES has experience with many tools to provide these services and will evaluate what the Commonwealth has available to recommend the best solution for you. As an example, we describe below how we use our Data Center Infrastructure Management (DCIM) tools in HPE data centers. The DCIM is a system management platform to address the management and monitoring of the physical data center layout (racks and cabinets) and associated cooling, electrical, and cable infrastructure. HPES uses DCIM tools to provide a consolidated physical asset database, including graphically displayed location information. HPES uses DCIM tools to provide a consolidated physical asset database, including graphically displayed location information, and to support the management of physical data center layout (racks and cabinets) and associated cooling, electrical, and cable infrastructure. **Facility Monitoring and Reporting** HPES' approach for data center infrastructure management is to leverage centralized monitoring and management, remote sensing, measurement, and intelligent controls. We propose

Ref#	Category	Question	Supplier Response
			following monitoring solutions to attain operational, system, and energy efficiency, including the following: • Sensing temperatures • Monitoring power • Monitoring rack conditions • Detecting fluid leaks • Intelligent control of precision cooling • Intelligent control of critical power • Managing alerts and alarms • Monitoring energy efficiency • Monitoring batteries • Monitoring and managing remotely. The data center monitoring system will enable setting threshold limits and reporting requirements and notification and escalation requirements, as well as provide performance measurement and monitoring requirements—such as fuel and water consumption, PUE/DCiE, etc. HPES uses the DCIM system for the integration of IT and facility management disciplines. The DCIM system will facilitate the centralized monitoring, management, and intelligent capacity planning of a data center's critical systems. Using the DCIM tools bridges the gap between the facility management systems (power, cooling, and the physical space) and the IT infrastructure management systems (compute, storage, and communications equipment) and provides visibility into the true capacity of the IT and infrastructure systems.
Q19.	MSI	The Commonwealth currently has a single traditional DR solution that requires the entire backup Data Center to be failed over. There is a desire to move to a more flexible solution that allows single Agencies or even applications to be failed over individually. This process requires design,	MSI's main responsibility is to make sure each supplier understands its role in the broader ITSCM (IT Service Continuity Management) program and plan. The overarching ITSCM plan would encompass all Commonwealth agencies and their critical applications yet would be modular enough to allow a

Ref#	Category	Question	Supplier Response
		development, operations, testing, and coordination. What role should VITA's MSI should play in this effort in relation with the Server Services provider?	reasonable level of autonomy to the agencies for testing their systems and applications. As a matter of best practice, it is to VITA's advantage to have a disaster recovery (DR) strategy tied to the criticality of each business application or grouping of business applications. DR testing can be scheduled at an agency level, for a group of applications, or at the data center level. Most DR service providers would prefer a data center level DR rehearsal or testing of a group of applications. It is possible to test a single application but is not a good use of time and resources. The process of declaring a disaster—even for testing purposes—requires advance planning and coordination of many different resources from VITA, the server service provider, and the MSI service provider to verify that there is no business interruption on the production site. To address a single application recovery, it is recommended that each application have a local resiliency measure to delay the failure. Local resiliency measures are techniques such server clustering, application clustering, and internal server component redundancies.
Q20.	Data Center	The Commonwealth is interested in Multi-site High Availability and Disaster Recovery Services. At a high-level, what do you recommend on the number and locations of centralized Data Centers the Commonwealth should utilize for that purpose? Any tradeoffs?	An important first step is to define the business rationale to establish a Multi-Site High Availability (HA) and Disaster Recovery (DR) Service? HA refers to the techniques and measures taken locally inside the production data center in order to keep the business applications available and on a green continuum. Application HA across the WAN and between two remote data centers is extremely costly and complex. Such measure is justified only when there are compelling business reasons and when the enterprise's business requires zero downtime for a particular application. As a matter of best practice, we recommend VITA leverage existing and/or develop new Business Impact Analysis (BIA) to

Ref#	Category	Question	Supplier Response
			rank its applications based on their appropriate Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). VITA's DR strategy needs to be tied to the outcome of the BIA. This approach justifies the investment in a particular DR strategy and makes certain that VITA is spending its resources wisely. Assuming VITA has done its BIA and an application HA across the WAN is justified, we recommend one production site and one recovery site.
Q21.	Migration	Suppliers will be required to provide an implantation plan to specify how they will take over responsibility for the existing environment. The Commonwealth is also interested in recommendations with regard to how the Commonwealth could migrate or transform to new Service offerings. What do you recommend for this migration plan?	HPES' approach is to develop a transition plan that defines the new service offering and its requirements. We will map the current environment to the new environment based on detailed information typically established through discovery assessment projects, which will identify the relationships between the applications and their dependencies, what platforms they reside on, business criticality, and functions. In addition, this plan will include business goals and requirements, risk awareness, contingency plans, and migration phases and timelines. HPES recommends that we set up the broker of services with public and private clouds so that we can begin to transition applications that are a good match for these platforms. HPES has services for application migration to the cloud and could identify those applications and functions that could be quickly moved to the new platforms. For more traditional platforms that might be long term the approach would be to review the refresh schedules of the HW. There are a few approaches—one is to purchase HW for applications that are on newer equipment and place it in our data center, move the application, and free up additional equipment to ship that can be used to move additional applications. The other approach is to walk in and take over and on refresh move to our data center, while we also move to public and private clouds. The early assessments of the environment will provide the data required to create the plan that will use the right mix of these strategies to address VITA's

Ref#	Category	Question	Supplier Response
			immediate goals. We have further details on our migration plan in Question 31.
Q22.	Enhanced Services	The Commonwealth is interested in receiving proposals to include new enhanced services, (e.g., Cloud, Analytics, Managed File Transfer) Can you recommend any other such enhanced services the Commonwealth should also consider including at the moment? How would you recommend these services be delivered?	Our experience suggests that today's technological landscape is shifting from an environment where data needs to not just be stored and shared, but fully utilized to make informed business decisions. This shift is especially noticeable in the public sector. No longer are agencies merely service providers—they are expected to create value for constituents by offering new services rapidly and efficiently. The role of data in Government has been elevated from simply a collection of information (now in digital form instead of ponderous paper files) to an arena where an agency can predict and shape future needs and respond to the real-time requests of citizens and employees. Agencies need to consider what it means to actually be a data-driven organization. Data-driven means fully capitalizing on all of the data available to your organization to make informed, data-backed decisions. Being data-driven means fully leveraging 100% of your relevant information—machine, business, and human—to create actionable insights that directly impact the business and mission of agencies. Public organizations must aim for this goal. Therefore, data analytics and data management services should be considered to assist agencies in discovering and understanding what constituents want, and tailor their services to meet these behavioral expectations. In addition to these data-driven services, we would also recommend the following services for VITA's consideration and inclusion: • **Applications Transformation to Cloud:** Provide VITA and its clients with a comprehensive overview of their applications, determine their suitability for cloud, develop a transformation plan, and migrate and modernize selected applications to the cloud. • **Cloud File Management:** A service for users to store, share, and synchronize files from any desktop and mobile device.

Ref#	Category	Question	Supplier Response
			Users can secure and control content at the file level with FIPS 140.2 encryption and digital rights management. VITA is provided administrative and support access to control user authentication and access, as well as to connect with their on-premises Windows File Shares and SharePoint sites. **Continuous Monitoring:** A proactive approach that compares the "as is" to the "should be" configurations of the network and all of its components to provide immediate feedback regarding where to focus action and investments. This approach automates network Information Assurance programs and makes certain that the information gathered is actionable and relevant—providing security insight and real-time status at all levels of Government.
Q23.	Enhanced Services	As the technology landscape changes in the Commonwealth's environment, could you describe other enhanced services that VITA and VITA Customers should consider in the future?	Most Government Agencies are heading toward a mix of private cloud, virtual private cloud, public cloud, and traditional IT resources. Hybrid infrastructure is a potential combination of these four elements across multiple vendors. The key to creating an optimal hybrid infrastructure strategy is to define the right mix of these deployment platforms specific to your agency's needs. Managed private cloud is ideal for mission-critical workloads that have specific security or compliance requirements or that require specific hardware to meet performance expectations while existing in any one of these models: Government-owned, contractor-operated; Government-owned, Government-operated; and contractor-owned and contractor-operated. A multi-tenant variation of Managed Private Cloud is Managed Virtual Private Cloud, a cloud in a managed environment that can scale quickly to meet agency requirements. Public cloud is ideal for cloud-native applications that have large variances in demand with a lessened emphasis on security. Traditional IT is best for supporting legacy applications that are not economically or technically feasible or too policy constrained to move to a cloud service platform.

Ref#	Category	Question	Supplier Response
			Hybrid cloud combines the distinct capabilities of private and public clouds. Enterprise IT can balance flexibility and control, while laying an architectural foundation that quickly scales services, speeds application development, and reduces IT costs. As we discussed, many public sector agencies are moving workloads to the hybrid cloud to cut costs and change cloud computing from a capital expense to an operating expense, where services can be purchased as needed. To prepare for such a migration we feel the following approach should be taken and requested of the supplier community. The first step in deploying an optimal hybrid infrastructure strategy is to define the right mix of IT—including private cloud, public cloud, and traditional IT. Private cloud is ideal for workloads that have specific security or compliance requirements or that require specific hardware to meet performance expectations. Public cloud is ideal for temporary workloads, workloads that have large variances in demand, or workloads that deal with public-facing information. Traditional IT is best for supporting legacy applications; applications that are not economically or technically feasible to move into a cloud platform; and for applications that have a very steady, unchanging demand profile. Hybrid infrastructure combines traditional deployments with public and private cloud resources, blending hybrid cloud with traditional IT. To determine the right mix each type of workload needs to be deployed on the best platform for its unique characteristics—considering cost, performance, security, regulatory, compliance, and other criteria. To define the right mix, the Commonwealth of Virginia (COV) needs to look at each application in its production inventory and analyze where that application would best be deployed based on the following:

Ref#	Category	Question	Supplier Response
			• Cost to migrate • Cost to operate • Regulatory requirements • Geographical requirements • Performance requirements • Security and confidentiality • Availability and reliability • Contractual terms and conditions. When thinking about individual applications the stakeholders must also assess what is cloud-compatible, what is not, and what is required to migrate an application to the cloud. HPES recommends that the Commonwealth include an option to assist with workload definition to assist with agency application transformations to the cloud. Although infrastructure is an essential component of any IT environment, applications are what actually run your enterprise and directly drive business value. The hybrid infrastructure provides the flexibility and agility to host any application—traditional, cloud, and future platform. Although the mix will change over time, this approach provides you with an end-to-end capability that is designed to adapt as you migrate existing applications, manage your sensitive data, and create new cloud native applications while reducing costs along the way. After defining your right mix, the second part of implementing a hybrid infrastructure strategy is powering the right mix by implementing a strategy with the right hardware, services, and partnerships. Any enterprise—no matter how large—will not have all of the skills, knowledge, and resources to implement and manage this complex, hybrid infrastructure strategy. A private cloud running the appropriate applications is a great place to start powering your right mix. By starting here an enterprise can set the standards that will be required for future

Ref#	Category	Question	Supplier Response
			cloud services. This also helps further define your right mix. When creating a hybrid infrastructure environment make sure your private cloud can directly integrate with your legacy environment, including the IT management tools. This is a critical step in creating a sustainable hybrid IT environment, not just a hybrid cloud solution. The next step in powering your right mix is to identify and start using public cloud services that meet application requirements appropriate for the public cloud. These services can then be selected not just on application fit, but also for a match to the standards and criteria set by the enterprise's private cloud implementation. It is critical to select and deploy the best solutions and right partners that have solutions-focused, end-to-end enterprise IT expertise that match the Commonwealth's defined hybrid infrastructure and hybrid cloud standards. Infrastructure, services, and partners need to be backed by global services, support, and a partner ecosystem. Partners that can bring cloud-skilled professional services with deep expertise in open source technologies are vital. Partners should also be certified in security, data management, and performance in order to effectively implement these types of comprehensive solutions. The right partners will help offer a more unified view of the overall hybrid infrastructure environment—for VITA and for end users of the hybrid IT environment. Optimizing your right mix is the ability to deliver effective administration of multi-cloud environments, workload migration, applications, data, users, compliance, and security. Optimizing your right mix should include the security, governance, and compliance required by the application and enterprise. It should regulate workloads and user access, provide on-demand provisioning of applications and workloads, and optimize resources across a complex open hybrid infrastructure. The advantages of optimizing your right mix are

Ref#	Category	Question	Supplier Response
			numerous and include delivering greater efficiency, meeting SLAs, facilitating compliance with industry and governmental requirements, increasing utilization of resources, and providing protection from security breaches. The resulting benefits are lowered costs, reduced risks, and greater productivity for the entire organization. Users should be able to seamlessly access the full complement of hybrid infrastructure resources specific to their job requirements. The service catalog should present to each audience (QA, developers, and testers) only the cloud and traditional IT resources that are appropriate and approved for their function. VITA needs to offer private and public cloud services that appear uniform to the customer, including the APIs that drive the services. The service catalog should present the options and differences of the services in an easy-to-understand manner. Systems administrators must be able to easily co-manage existing legacy IT resources as well as private and public cloud resources from a single pane of glass. They also need a way to virtually move assets from the legacy environment to the private cloud as resources are freed up. With the right management tools you can achieve the following: • Support security, governance, and compliance requirements. • Administer and optimize resources across a hybrid infrastructure to minimize costs and maximize utilization for internal and external services. • Verify that your service meets performance expectations. • Provide metering, showback, and chargeback for internal budgeting and controls. • Control data locality to deliver ultra-low latency performance. As a result of needing to have a hybrid environment to support

Ref#	Category	Question	Supplier Response
			the needs of the agencies and to support their workloads, it is critical to have a platform to be able to manage this environment across multiple suppliers. Therefore, we strongly recommend that VITA include a Request for Service Broker or Cloud Service Broker Services. A Service Broker provides a suite of managed services to enable agencies to provision, control, and manage multiple vendors from a fully integrated view. One of the big advantages of leveraging a hybrid IT Cloud Broker system—which rides on top of all of these platforms and normalizes them—is that it provides total oversight into all aspects of IT management that also allows you to make intelligent decisions, so that you are not leveraging just one provider and forcing that one provider to meet all of your needs. If executed correctly a Service Broker approach offers an integrated view of your hybrid IT ecosystem.
Q24.	Enhanced Services	What would you propose as a good business case for virtualizing the desktop (offering VDI)?	Several factors can contribute to a business case for establishing a virtual desktop environment as follows: • **Data Security** – The best business case for virtualizing a desktop environment a compelling need for data security, because a correctly configured virtual desktop infrastructure (VDI) offering will safeguard that environment, keeping all data in the data center and off of individual devices. Such an environment provides security for personally identifiable information (PII) such as data collected and maintained within the Commonwealth. • **Any Device, Anytime, Anywhere** – Another aspect of a virtual desktop environment that gives impetus to the business case is the “any device, anytime, anywhere” capability available for VDI environments. If VITA desires it, then the properly configured VDI environment can provide end users with access to their data, projects, email, whatever they need—based on VITA’s direction—to do

Ref#	Category	Question	Supplier Response
			their work wherever they are and on whatever approved device is chosen. There are many options available for this aspect of VDI. Basically, it can be as restrictive or as flexible as VITA wants it to be. • **Reduced Support** – Another aspect of VDI that lends support to the business case is reduced support in two main areas: (1) Reduced effort required to maintain desktop images, and a corresponding decrease in the required infrastructure to support ongoing maintenance activities for desktop image support. A common image can be configured and maintained within the data center, then shared among as many users as desired. Alternatively, the same image can be deployed to many different virtual desktops at boot time if a full desktop environment is needed or desired. (2) Reduced on-site support labor to support end-user devices. IMACDs (Installation, Move, Add, Change, and Disposal Services) can be significantly reduced. • **Adoption of New Desktop Environments** – An increasingly significant factor in favor of VDI deployment is the ease with which it supports the rollout and adoption of new desktop environments, such as Windows 10. Essentially, the new desktop is established within the data center, and the users simply boot to the new environment when it is available.
Q25.	Data Center LAN	What do you recommend as the best demarcation point between the Data Center LAN and the Network or WAN? The Commonwealth wants to make the cleanest scope separation for a future WAN Network RFP.	The demarcation point between Data center LAN and WAN services should be at the Customer Edge Router (CE) within the data center. Typically a CE router is the natural operational demark between suppliers who provide Data Center services and those suppliers that provide Wide Area Network(WAN)/Metropolitan Area Networks(MAN) transport infrastructures/services. Although the management realms are separate with regards to the physical assets, the services provided by both need to be collaborative to provide a holistic end-to-end view of service management. **Accordingly, HPES recommends the separation of WAN/MAN**

Ref#	Category	Question	Supplier Response
			and Data Center LAN services. WAN/MAN services are traditionally provided by carries who have the infrastructure and provisioning relationships with TELCO's/Local LEC's needed to provide transport provisioning outside of a data center proper. This operational demark typically requires different types of business relationships with different technologies, skill sets, management, and monitoring multi-tenant toolsets. As virtualization, hyper-converged and Software Defined Networks become more prevalent and more reliant on local assets within a data center architecture, the demarks between data center services and WAN/MAN transport become natural operational handoffs between the suppliers of these services. Provisioning of virtualized workloads from the automations dependent on Data Center assets e.g. LAN (virtualized switch fabric), Storage (FCoE, iSCSI, direct) and Security (IDAM) suggest these dependent services reside in the tower (supplier) that understands these inter dependencies.
Q26.	Data Center LAN	In the current RFI, the Commonwealth has bundled Data Center LAN services (e.g., switching, routing, load balancing and firewall) with Server and Storage services. Do you find any challenges, issues, or concerns with this approach and why? Any recommendations?	The approach adopted by the Commonwealth of bundling the data center LAN services with the server and storage services is in line with data center virtualization, implementation of converged infrastructure, and hybrid infrastructure models. As these services become virtualized, the lines between network, server, and storage support become blurred. If we take the emergence of DevOps in the past few years as an example, we can draw a similar conclusion as to what the operating model will be between LAN, server, and storage services. It is important that engineering and operation teams are cross trained in all three service areas. We would recommend that the Commonwealth include minimum skill requirements for the key positions in those areas. Having a team that operates a multi-tenant data center infrastructure with hybrid services and that is able to leverage experience designing and operating those centers would benefit the Commonwealth in reduced time to implement and reduced

Ref#	Category	Question	Supplier Response
			operation cost.
Q27.	Data Center LAN	The Commonwealth did not bundle Data Center LAN services (e.g., switching, routing, load balancing and firewall) with the Data Center Facility services (e.g., HVAC, power, raised floor). Do you believe this is the correct approach? Do you have any recommendations?	The Commonwealth's approach aligns with the recommended solution. While the two support teams will share an integrated monitoring toolset as indicated in Question 18, separating the data center facilities services from the bundled data center LAN server and storage services will lead to higher levels of services, as each team will focus on optimizing the services provided. Facilities management leverages resources that provide services such as physical security, HVAC, electrical, and fire suppression systems. They achieve efficiencies providing those same services to multiple customers. They use building management toolsets) for monitoring, managing, and maintaining the facilities, so they are consumers of IT services. At the same time, data center LAN services leverage their resources to manage the IT component. Even when they exist in the same company, these services are under completely different management and operation teams.
Q28.	Data Center LAN	The Commonwealth is considering decoupling the Data Center Facility services from the Server, Storage, and Data Center LAN services. What do you think of this approach? What do you think are the advantages, disadvantages and tradeoffs of splitting the facility services out versus coupling these services with Server, Storage, Data Center LAN?	The approach followed by the Commonwealth is in line with the recommended solution. While the two support teams will share an integrated monitoring toolset as indicated in Question 18, separating the data center facilities services from the bundled data center LAN server and storage services will lead to higher levels of services, as each team will focus on optimizing the services provided.
Q29.	Data Center LAN	Supplier is expected to provide centralized Data Center LAN services. Should LANs in non-centralized Data Centers be part of the scope for Data Center LAN services or bid as part of Network/WAN in a future procurement? What would be the pros/cons and tradeoffs?	All network services (LAN and WAN) for all data centers (centralized or non-centralized) should be integrated with the data center server, storage, and security services. We detail in Question 25 the reasons why LAN and WAN services should be integrated so as to achieve higher efficiencies (operational, SDN plus NFV for optimum traffic, and application integration), control (use of network of host-based overlay technologies), and flexibility (data center extension, workload placement, multi-tenant).

Ref#	Category	Question	Supplier Response
			Providing the same support for centralized and non-centralized data centers will provide uniform overall network architecture, enterprise security enforcement, and easier migration to common services and hybrid services as well as leverage expert knowledge, best practices, and resource allocation to support surges, special events, and improved DR response.
Q30.	Data Center LAN	If the solution includes new Data Centers, who should provision and manage the network connections between the Data Center locations? Should it be the Network Provider, the Data Center Provider or the Server, Storage, Data Center LAN Provider?	The Data Center LAN and WAN services should be separated as indicated in our response to Section 25. Data Center LAN services should be integrated with data center Server and Storage services as indicated in our response to Question 26 . The provisioning and management of the network transport between data center facilities should be managed by the provider of those transport mediums (WAN/MAN suppliers).
Q31.	Data Center	How does the Supplier propose to migrate Server, Storage, Data Center LAN services out of the CESC datacenter by June 2019 or earlier? Describe how the Supplier would seamlessly migrate out of CESC like-for-like, transform to new services, or a combination of the two? What are the recommended approaches?	HPES will provide the Commonwealth with a technically qualified, technically accredited data center migration experienced staff with the required security clearance. Our staff will have a deep understanding of the following concepts: • Server, storage, data center and LAN data center infrastructure migration • Discovery assessments, to identify the current hardware and software environments • Data migration solution designs within heterogeneous infrastructure environments • Hardware, software, and technology upgrades in support of data migration. HPES recommend approach includes the following: • Discovery assessment • Migrate low-risk to high-risk applications based on business objectives • Design

Ref#	Category	Question	Supplier Response
			– Business department and application phases approach – Risk assessment and management – Capacities accuracy – Contingency and test plans. In collaboration with the Commonwealth, HPES will propose engaging a hardware/software infrastructure discovery assessment service to identify and determine the environment and data center migration concerns and issues that may negatively impact stability, availability, performance, and efficiencies. This assessment will provide HPES with an overview of the server, storage, data center, and LAN environment to help establish a baseline design for migration to the new data center in support of Commonwealth goals and business objectives. HPES will apply the assessment information and data captured during the assessment as the foundation for the data center migration design. We will leverage best practice knowledge and experience to design the best phase-in approach migration solution with emphasis on contingency plans and schedules that facilitate non-disruptive operation. The HPES dedicated data migration staff will then perform the data center migration per the agreed Commonwealth design approach, schedules, and required reporting. Multiple regional data centers exist in the current state, lacking standardization, growth, and scalability. Migration of data center IT systems and applications is a highly strategic project that must be executed without impacting operations, service level agreements (SLAs), and data protection requirements. The migration strategy should take into consideration that the applications and data in the production environment are changing consistently and being replicated to a remote DR facility on a regular basis. The migration strategy for the data center IT systems and applications will make sure that optimal costs are incurred on server, storage, network, and applications hardware and

Ref#	Category	Question	Supplier Response
			software usability. The migration program will make certain that the project phases in deploying the right resources and minimizing risk to operations. The team will determine system Recovery Point Objective (RPO), system availability objective, and system Recovery Time Objective (RTO). The migration team will use appropriate tools, technologies, and processes as well as ITIL and industry best practices. The migration team will perform application and infrastructure analysis and identify key contacts. The team will compile the application profile, infrastructure profile, and facilities profile and will use established tools to determine application interdependencies. Based on the compiled information about the applications and infrastructure, the team will design the hosting infrastructure physical, virtual, or hybrid data center based on custom and shared infrastructure resources and services. The team will perform virtualization and assessment of servers, taking into consideration specific software requirements and application-specific appliances. The team will also review LAN/WAN network connectivity and security requirements. They will build and conduct pilot tests to evaluate move bundle packages. The team will conduct unit testing, system integration testing, and network performance testing.
Q32.	Cloud Services	The Commonwealth is interested in a solution that integrates traditional hosting services with new private, community, and public cloud offerings. How do you propose integrating these services?	More and more, enterprises recognize that the cloud is a driver for cost savings, flexibility, and agility in maintaining mission effectiveness and responding to rapidly evolving global threats. Cloud computing radically changes the way infrastructure, applications, and information are sourced, consumed, and managed. Enterprises are not just building internal infrastructure and services; today, they need to broker or consume internal and third-party services across a spectrum of service providers. To achieve maximum value from their applications and IT investments, enterprise leaders must have visibility into the

Ref#	Category	Question	Supplier Response
			cost, performance, compliance, and availability of their systems. Most organizations have started to transform their IT environment from the traditional data center model to a hybrid delivery model including cloud. Many are faced with complex and aging environments and applications portfolios, and struggle with lack of experience, tools, and know-how to transform their workloads and business processes. They want to embrace the cloud while protecting their current investments, but need help in planning, implementing, and managing the entire journey from development to testing and operations. Market analysis shows that many clients have started on this journey and plan to accelerate adoption of private and public cloud in the near future, while still retaining some critical traditional IT services. Enterprises are looking for ways to mitigate the chaos of acquisition, procurement, and management of all their cloud and non-cloud service providers. Their challenges include the following: • IT services cannot keep up with the pace of requirements to innovate and support the business • IT spend and performance is disjointed and "siloed" – No visibility into true service cost or capability alignment – No common set of metrics to evaluate services and costs of providers/services – No ability to manage workloads that run across multiple providers – Minimal visibility into cost and performance of providers • Security and compliance exposure risk is prevalent as a result of "shadow IT," where departments use their own, often unsecured, cloud services • Services are disjointed with minimal lifecycle management

Ref#	Category	Question	Supplier Response
			and automation • Compliance and data security are difficult in hybrid cloud environments • Extracting maximum return on investment (ROI) from traditional IT during a migration is challenging. Likewise, the VITA contractor needs to provide fully integrated multi-cloud analysis and orchestration for its external Cloud Service Providers (CSPs), on-premise managed cloud services, and on-premise virtual and physical infrastructure. It needs a single integrated orchestration solution to prevent cloud vendor lock-in (i.e., vendor or technology dependency) and enable automation and service orchestration while evaluating the potential security, risk, cost, and functional benefits. Cloud Broker solutions are designed to provide governance over a collection of varied IT and cloud service providers, control shadow IT, and establish service efficiencies by giving a single view of enterprise IT spending, service provisioning, internal usage patterns, and unified governance. Working with our partners, a cloud broker solution provides a management platform and IT service marketplace that offers single-portal access to hybrid cloud service providers and their services. This solution includes the following: • Service catalog and subscription management • Financial and asset management • Performance management • Security and compliance management • IT Service Management • Compliance management • Service provider interfacing • Administrative services for the management of users, policies, configurations, and security settings.

Ref#	Category	Question	Supplier Response
			Cloud broker solutions use a high level of automation and orchestration to integrate and manage across hybrid clouds and the traditional data center and can also interact with services and processes that are manual or semi-automated.
Q33.	Cloud Services	What would be the best practice with regard to Suppliers owning the cloud contracts and potentially transferring that contract to the Commonwealth? Should the Commonwealth own that contract outright? Are there any other alternatives to be considered?	Many cloud service providers (CSPs) do not provide the SLAs or enterprise-class support that large organizations are accustomed to purchasing. Enterprises often turn to resellers of these CSPs to deliver the level of service that their applications and workload demand. In these situations, it is most common for the reseller of the CSP to own the contractual relationship with the cloud vendor. This arrangement simplifies contracting for the Commonwealth by allowing it to focus on a service that is fully consumable by its entities and also enables the supplier to introduce new and innovative solutions for the Commonwealth without requiring that it go through a sometimes lengthy contracting process of its own.
Q34.	Cloud Services	When the Commonwealth buys cloud services offerings how do you propose to identify where the data and services are located?	Several factors should be considered when selecting the location from which Commonwealth data and cloud services are delivered, as follows: • First and foremost, all applicable privacy and export control laws and regulations that pertain to the data being stored must be reviewed and complied with. This applies not only to the location of the data center, but also to the capability of the CSP to provide the necessary controls required to protect Commonwealth data. • Next, network latency should be considered. In most cases, leveraging a cloud service in close proximity to end users can reduce network latency and provide a better user experience. • When deploying workload to the cloud, it is sometimes necessary to collocate physical servers or specialized appliances along with the application deployed in the cloud.

Ref#	Category	Question	Supplier Response
			In these cases, it is important that the CSP offer collocation services organically or offer such services through a partner located close to the CSP's data center. • When considering disaster recovery, a balance needs to be struck between sufficient geographic separation to make certain that both sites are not impacted by the same event and the network latency issues that will arise after failover if the DR site is too far from the end users.
B.	**Financial/Server Storage**		
Q35.	Pricing Structure	The Commonwealth is interested in creating the best possible pricing structure for the Services. In light of that fact, Supplier is invited to both comment on the structure described in Exhibit 4.1 and 4.2, and to propose an alternate pricing structure if they believe that it will better serve the interests of both parties. The Commonwealth will contemplate any proposed pricing structure along five dimensions: 1. **Predictable:** To the greatest extent possible, customers should be able to forecast charges ahead of time; changes in pricing that occur over time should not be a surprise. 2. **Manageable**: The pricing should not be so complex that it is needlessly difficult to administer. If quantities of work or equipment in the environment must be measured, then those quantities should be as easy and transparent as possible to measure. 3. **Fair:** The service pricing must be a reasonable proxy for a services provider's underlying costs and should adequately recover those costs. Additionally, to the extent possible, the party that causes any incremental cost should bear that cost.	The price table segregates Resource Units (RUs) by operating system (OS) type and level of service, but not by size or virtual/physical servers. As we have discussed in our answer to Question 7, we recommend a Service Broker approach, including a catalog that will identify the items that need to be included in the pricing structure. We recommend expanding the RU list to include various components described as follows so that there is a flexible methodology for obtaining the services that meet the specific needs of the service or application being supported. The catalog is configured to meet the Commonwealth's requirements to be predictable, manageable, fair, and flexible and incentivizes users to size their environment to exactly what they need so that costs are kept in line. The service levels described in Question 6 would also be applied to have an end-to-end price for the service offered. **Hardware** (Monthly charge per device) • One per standard orderable device configuration • Predefined hardware configurations (Small, Medium, Large, Extra Large) • Have CPU and RAM as orderable uplifts for more flexibility • Includes hardware, lease charges, and hardware maintenance

Ref#	Category	Question	Supplier Response
		4. **Incentives:** All pricing structures will incentivize certain behaviors and discourage others. The goals of the sourcing program must be kept in mind when considering the behaviors that might be driven by a pricing structure. For example, a goal to encourage server consolidation might include reduced cost at a centralized data center. 5. **Flexible:** As consumption moves up and down, the charges should also adjust. Technology is an evolving industry, and the ability to turn down an old service to turn up a new service is one of the benefits of an efficient IT sourcing agreement. Such adjustments may include minor volume changes month to month, significant scope additions, reductions, or terminations, and ability of large service providers to re-deploy investments.	• For virtual machines, each virtual includes a fraction of underlying hardware cost **Hardware Installation** (One-time charge) • One per standard orderable device configuration **Software:** One-time charge or monthly charge based on license type and defined in the catalog: • One per software license (e.g., Oracle, SQL Server, Windows, Red Hat) • It is important to clearly define the licensing unit and provide guidance in the Service Catalog on how to order based on the hardware configuration or whatever the license multiplier is. **Support Services** • **Level 1:** includes facility charges (KW rate, basic smart hands)—at a quantity based on KW rating – Can optionally include an allocation of data center network costs (both HW and SW) • **Level 2:** includes base managed services (labor only): system administration (different RUs by OS)—with a quantity of 1 per OS instance). Note that there is no difference between physical and virtual servers. This involves the following: – This approach can be extended to network devices, based on standard key performance indicators (KPIs) (if specialty network equipment is involved and you are not charging for network at Level 1), – If the contract will require refresh, you can include this labor cost here (some contracts charge it separately; some include it). • **Level 3:** Managed services uplifts (labor only—different RUs by type—client orders as many as apply, at quantity of 1). This includes the following:

Ref#	Category	Question	Supplier Response
			– Database management – Application monitoring – Middleware support – Batch processing – High Availability (clustering/load balancing) – Includes installation of the product/service, but not the license itself. Cloud services would have their own listing of services based on the consumption model chosen. The Service Broker solution enables a manageable methodology for requesting services and tracking the charges per customer within the chosen toolset, so that reporting and chargeback are easily managed. This methodology also supports predictability because the prices for each service are clearly documented so that if a customer plans to expand their platform they can easily see what the costs would be to support that expansion. The pricing is fair because a customer only pays for what they need—if they need a small server then they pay for that as opposed to a model with only one-size server, where they may be paying for more than they need. Incentives can be built in as mentioned by passing cost savings on to the customer for more cost-effective solutions—(i.e., virtual versus physical servers and cloud solutions versus dedicated).
Q36.	Inventory and Volume Collection	The Commonwealth is interested in introducing new Resource Units that do not exist in the current contract; in order to fairly compensate Supplier for service delivered, and support the other goals described in question 36, Supplier is asked to describe their experience and approach to collecting and verifying volumes both before and after contract signing, and the approaches they use to adjusting financials in the event that the initial count is incorrect. For example, today database support is provided by the	HPES recommends establishing a baseline upon contract award based on the current incumbent's data. Upon award we follow a defined process to validate that baseline—and, if necessary, re-baseline to match the actual environment. Our asset management process will allow us to collect and verify this information, as described below. We can track hardware and software assets following the same processes using the tools appropriate for the asset type.

Ref#	Category	Question	Supplier Response
		Supplier, but is not separately billable. The Commonwealth sees an advantage to separating out database support and making it a separate chargeable unit, how would the service provider collect and verify the volumes to support this chargeable unit?	**Months 1–2** • Begin formally reviewing contract and due diligence documentation according to our project management methodology to establish deliverables, risks, assumptions, and gaps. • Engage asset management resources. • Validate Statement of Work requirements. • Conduct a process integration activity among our customer, HPES, and third-party service providers to establish business rules and processes to support asset management services. • Define reporting requirements. • Validate and confirm critical data elements to be tracked in the asset repository. • Define asset tag requirements. • Develop a Statement of Work for the physical inventory. • Install tools aligned with configuration and implementation of HPES common tools and processes and the Service Desk. **Initial Asset Inventory** Before the start of steady-state asset management support, HPES performs a complete inventory of in-scope IT hardware/software assets. This information is captured during a physical visit to all locations with more than 25 seats and by an approved mail-in or Web-based process to remote locations with fewer than 25 seats. Each asset record consists of associated profile data elements, combined to represent the description of an individual business asset or user at any point in the asset's life cycle. An asset repository tool assimilates and reports on the content of the inventory data to facilitate accurate chargeback. An auto-discovery tool assists in tracking the number of software licenses. Actual inventory is uploaded into the asset repository and

Ref#	Category	Question	Supplier Response
			managed throughout the contract with links into the Service Broker solution to add assets as procured.
Q37.	Asset Ownership	The Commonwealth consumes certain services today which are underpinned by a set of assets (servers, firewalls, etc.). The Commonwealth (or their designee) has the right to acquire these assets. The Commonwealth has a desire to consume services; rather than own assets, and envisions Supplier acquiring these assets and using them to provide services back to the commonwealth. Please describe experiences acquiring assets from an incumbent, and also describe your recommend financial treatment of their cost recovery for these assets.	HPES has access to—and a close working relationship with—HP Enterprise Financial Services (HPEFS). HPEFS is able to buy legacy assets and lease them back to HPES. HPEFS would perform a valuation of the legacy assets and provide the resulting lease cost that would then be included in the monthly RU service price offered by HPES.
C.	**Managed Security**		
Q38.	Security	The Commonwealth's Managed Security description of services includes all the required scope bundled for a single experienced Security Supplier. Do you see any challenges or issues with this bundled model?	HPES has experience delivering managed security services as described in this request for information and believe it would be in the Commonwealth's best interest to take this bundled approach. We believe that it is critical for the selected managed security services provider to have full visibility into and management of the security posture of the entire VITA environment. This includes centralized data capture, dashboards, and other best practices that fully take advantage of the single provider's experience and translates it into visible and transparent indicators of their ability to meet and sustain the required security posture of the infrastructure, components, communications, personnel, and processes within the customer's control. HPES always takes into account the use of standards and practices and rapidly evolving national, regional, and international regulations regarding the protection of systems and data as well as the integrity of controls and protection processes and platforms associated with each instance of a program. We are confident that a single supplier with the experience, insight, and overall historical knowledge of the challenges facing

Ref#	Category	Question	Supplier Response
			the Commonwealth would likely best serve the interests of all of the program's wide range of stakeholders.
Q39.	Security	Do have any concerns or recommendations regarding how to scale Managed Security Services to organizations of the size and complexity of the Commonwealth?	HPES looks at the challenge of scale and scope from the perspective of our experience. This allows our team to readily recognize similar patterns for scaling implementation of managed security services across enterprise and even global boundaries. To establish the value of this perspective, we readily incorporate it in the earliest stages of design through to procurement and expansion of infrastructure and logistics and eventually into its production and sustainment mode of operations. Understanding this lifecycle approach helps us confidently recommend that you start with the security functions/techniques, tools, processes, and procedures you have in place. Evaluate each process and project its use and development to maturity and ultimate replacement, providing a consistent level of predictable, repeatable process standards and practices to govern the overall program. Once the tempo and pace of the program have been established, teams can readily expand from there to create a full range, passive→ proactive, network defensive posture provided in an environment and with scalable tools and architecture that enables full testing, assurance, risk management, and compliance. HPES recommends a stance of openness to new technology adoption and best practice integration along the full lifecycle and outlined in the projected milestones of the evolving program's roadmap toward the future.
Q40.	Security	Can you provide examples of comparable environments where you offer security services similar to those required by the Commonwealth?	With nearly 50 direct, or nested, clients, most environment types and sizes are represented. HPES provides or has provided just about everything from a 16-server file-sharing environment to a public cloud-based healthcare market, with elastic load

Ref#	Category	Question	Supplier Response
			balancing. This experience is backed by nearly four decades of expanding and evolving security practice and technology leadership, including a current cadre of personnel and experience credentials that includes the following: • 5000+ security professionals manage more than 10,000 enterprise clients Over 3,000 security specific researchers • Over 6,000 firewalls, 3,000 IDS and 800+ state, local, and federal agencies with ongoing deployed IAM platforms • Historic abilities to secure over 1 million applications and 2.6 billion lines of code • Active detection and quarantine of over 45 million instances of malware • Efficient handling of 23 billion security events each month • Greater than 75% of the world's financial companies use HPE enterprise security services • Monitoring and sustainment of over 500,000 managed security devices • Protection of over 47 million secured accounts Given this historical performance, we believe that these credentials form only the first step in establishing our credibility as the managed security provider of choice among our client base. Further examples across government and industry—readily available with minimal research—help testify to the depth of HPES' experience and the breadth of areas in which we are now recognized leaders for public sector entities in protecting, preserving, and sustaining the confidentiality, integrity, and availability of their mission-critical data.
Q41.	Security	Have you supported Managed Security services in distributed environments - both physical and virtual including on premise and off premise implementations?	Yes, almost all of our clients have a combination of physical and virtualized servers. This includes both on-premise and off-

Ref#	Category	Question	Supplier Response
			premise client environments.
Q42.	Security	Do you offer solutions supporting geographically diverse locations (e.g., remote location with satellite)?	Yes, this describes approximately 30% of the client base we currently support. Additionally, we have customers based exclusively outside HPE data centers.
Q43.	Security	How have you implemented solutions similar to those in the Commonwealth making use of a centralized federated environment?	Centralized federated environments can come in two flavors. **Example 1: Centralized Federation Toolsets** **Industry Solutions: Financial, Government, National Security and Industrial/Infrastructure Implementations:** Each of our internal client implementation examples has been using a Centralized Federation toolset. This is generally implemented for one organization/entity where there is direct connectivity to Identity Providers (IdP) authenticating data sources. This reflects the traditional requirements and capabilities for use of most centralized access management tools. **Establishing Trust Through Centralized Federation:** Our experience demonstrates how Identity Providers and Service Providers (SP) establish "trust" through this single centralized federated system. This centralized federation manages the authentication of users to the trusted SPs/relying parties, signing and passing assertions or claims to the SPs for authorization or for customized content to their application. **Example 2: Extended Centralized Federation Broker: Geolocation Diverse Operations, Subsidiary Commercial Management, Judicial and Financial Sector Operations Security Across Centralized Agency, State, and Local Data Sharing-Enabled Systems Protections and Authentication and Federal, State, and Local Agency Collaborative Environments:** Another is an extended centralized federation broker or hub that typically includes organizations or agencies outside of the immediate organization and with no direct connectivity to their

Ref#	Category	Question	Supplier Response
			user repositories. *Note: This type of solution would normally not store identities, except for a unique identifier with account-linking.* **Facilitating Pass-Through with Trust Validation and Platform Redundancy, Creating Identity Unification and Adaptation, without Losing Integrity of Session Authentication and Identity Management:** This process enables a pass-through, where this centralized federated broker or hub acts as a central SP and establishes trust with multitudes of IdPs, receiving their assertion and claims through one protocol, such as SAML. Then, the federated hub or broker will become the IdP and perform Identity Provider aggregation, proxy, and protocol translation (SAML, WS-Fed, OpenID, OAuth, and Open ID Connect) to downstream service providers. **A Future That Includes a Broad Range of Networking and Operational Schema Options for VITA:** To support VITA options—near term and long term—our team can leverage established experience with current federation approaches and future development of the federation concept across the on premise and cloud delivery mechanisms and architecture.
Q44.	Security	What do you consider to the be the key challenges and tradeoffs for the implementation of Managed Security Services in an environment similar to the Commonwealth?	**Challenges and Tradeoffs Relevant to MSS Implementations:** *Managed Security Implementation Challenge #1: Distributed and collaborative it environments require assured identity that is flexible enough to meet current and future operations models.* In extension to our answer found in Question 43, as part of our team's IP, Knowledge Base and in working with public/private cloud industry partners, we recognize the challenges associated with cloud-based access authentications associated with transitioning to this type of service delivery model. For example and as a part of your transformation journey, our combined team and cloud partners' Identity and Access

Ref#	Category	Question	Supplier Response
			Management (IAM) cloud solution services will actively address the challenges that present themselves in three primary areas:. • Managing identities and their life cycle. Enterprise users must be provisioned and de-provisioned in a seamless and integrated manner. Access must be revoked across all granted systems. • Federated Single Sign-On – To interoperate across organizations and agencies, the IAM service provides federation functionalities acting as an Identity Provider and a Service Provider. • Strong Authentication delivers on multifactor requirements. Examples include using OTP and PKI, but can be expanded to include risk-based models, such as device ID and geolocation. *Managed Security Implementation Challenge #2: Assessing value of the information and the mandates needed to protect it within your MSS implementation and technology planning.* The key tradeoffs made across MSS implementations are driven by the acceptable risk level established by the customer environment, and this includes the following: • Understanding the open data market value (sensitivity and monetary value to the dark market) of the data residing on systems. This is especially important when handling Personal Identifiable Information (PII). This is often the most overlooked item when establishing the levels of control and protection surrounding what may be treated as commonly held data within Government organizations and agencies. • Ability to Meet Regulatory Mandates – Adhering to architectures and processes determined by third parties such as Government organizations for the handling, protection, monitoring, alert, response, and remediation. This includes data types like PII, HIPAA, PCI-DSS, Law Enforcement Sensitive, and other

Ref#	Category	Question	Supplier Response
			regulated information that has oversight and controls. In these cases state sovereign immunity may not be sufficient to protect state personnel or agencies from civil or criminal actions for negligent handling of this type of data. *Managed Security Implementation Challenge #3: Assessing and examining a full range of options that balance budgetary and operational management of information security against the growing potential for automation—leading security professionals to have to choose versus staffing solutions to monitor and respond to security incidents over the life of the program.* **Establishing Expectations with Stakeholder, Data Owners, and Citizens of the Commonwealth:** This third challenge is far from the last, but the previous three are the most common discussions from a policy perspective that ultimately drive the resource and infrastructure budgeting commitments that the Commonwealth will be making as it describes the needs for MSS as part of an integrated services, storage, networking, and hosting set of platforms and services. As with many challenges facing security planners in the information age, there are a multitude of different ways that industry, Government, military, and law enforcement view the priority and resource availability mix that is at the heart of their decision process for adopting new MSS platforms and the extent to which those platforms' feature and function sets provide a reasonable set of tradeoffs while continuing to provide the security value and performance necessary to meet the expectations of the program's stakeholders. **Examples of Similar Situations and Solutions:** **Central Platforms and Central MSS Management** At one end of the resource-based spectrum is the establishment of single fixed centralized controls, data environments, and

Ref#	Category	Question	Supplier Response
			operational platforms. This has been a legacy architecture-based solution for many state and local agencies that seek to leverage their long-term investments in infrastructure and apply them to new processes and possibilities that support IT requirements for their agencies, citizens, and supporting vendor communities. The key benefit of this type of single premise and on premise solution set is that it simplifies locations and leverages current assets, if available. It provides a continuity of operations that understands the logistical and transportation, technical, and networking challenges of the fixed location and readily identifies the related security challenges based on physical, operational, logical, and environmental factors at the on premise solution site. The key challenge as an on premise only solution is the ability to match local talent and skills or have the ability to coordinate staffing and relocation plans for teams are the key considerations that we have seen in these implementations. This is especially important in the MSS world, where 24x7 operations are the norm for monitoring, managing incidents, and conducting remediation and post-incident activities. Again, sites that exist already will require a ramp to find qualified talent in that location, as well as the same for any similarly designed DR or Continuity of Operations (COOP) site. As such, although operational and cost of infrastructure may decrease and the ability of the Commonwealth to gain greater lifespan from existing facilities, it faces the equally daunting challenges of finding and maintaining the new and highly sought-after skill sets in the target location. The need to move or hire locally may drive toward higher overall operational and human resource budgets and total cost of ownership. These challenges may or may not occur in the widely adopted alternative, the establishment of a potential leveraged solution for MSS activities.

Ref#	Category	Question	Supplier Response
			Leveraged and Distributed Solutions for MSS Management Leveraged solutions take advantage of the wide geographic diversity of well-established, modern, and ongoing improvement-focused facilities. These facilities understand the ongoing multi-faceted security risks to information and the confidentiality, integrity, and availability that are critical to maintaining the public trust in the agencies that hold citizen and agency-sensitive data. Leveraged solutions rely on consistent and continually updated security procedures and processes; adherence to all national, state, local, and international standards for performance; and provide a menu of options that integrate with the tempo, sensitivity, and criticality of the data and mission of the systems platforms that they protect. **Leverage and Agility Meet at MSS Delivery and Response** For many teams, they believe that MSS-leveraged environments only refer to specific monitoring and control centers. These centers are located at locations that are designed to be physically secure and hold reasonable sets of educated and qualified populations that are the basis for long-term career development of the teams that operate there. The centers benefit from the speed and security of modern networking capabilities to take care of the core functionalities for protecting data through careful evaluation of performance, behavior, and operational characteristics of the systems; analysis of logging, IAM, and user information; and a vigilant 24x7 watch over the environment. Leveraged MSS benefits from being logically integrated, yet physically separate from the site—providing a comprehensive and constant watch on the information and systems it is designed to protect. Automation, sensors, systems analytics, and dashboards and Security Operation Center (SOC) activities work in concert to maintain the level of detailed examination that is so critical to early detection of threats, both internal and external; new

Ref#	Category	Question	Supplier Response
			malware or zero-day risks; platform compliance monitoring; and complete auditability from a dedicated and distributed team that is fully prepared to meet the DR and COOP scenarios that may face the Commonwealth. For that reason, our experience has shown that overall long-term costs fully mitigate these initial uplifts—initial one-time costs for aligning leveraged services to the mission, tempo, and regulatory requirements of specific agency platforms, enclaves and shared data and risk management domains—and provide a consistent level of predictable, protective budgeting and performance-related metrics to demonstrate clear results for the Commonwealth's stakeholders.
Q45.	Security	What do propose at a high level to be the key strategies and implementation elements of any typical security services solution migration?	HPES conducts migration by phase to provide optimum security coverage and reduce risks of coverage gaps during transition—Security Incident and Event Management, Data Loss Prevention, Vulnerability Management and Vulnerability Scanning. Migration in this sense also assumes that client security toolsets stay in place *unless* the client wants to review current and new options.
Q46.	Security	Can you recommend additional Managed Security Services that are not currently included or considered in the scope of described services?	Yes, regular penetration testing (at all relevant layers); security architecture and maturity review; Identity and Access Management services; incident response retainer (if not in place or if there is no incident response team local to client to stop a breach); advanced persistent threat (APT) monitoring and hunting – to include threat intelligence feed if none exists.
Q47.	Security	Based in your experience, what are the key challenges with regard to the regulatory requirements included in the scope of services? Do you have any recommendations based on your experience?	Key challenges include determining which security standards—Health Insurance Portability and Accountability Act (HIPAA), Federal Financial Institutions Examination Council (FFIEC), Payment Card Industry (PCI), Federal Information Processing Standards (FIPS), etc.—apply to the information and systems we protect then applying those regulations or guidelines appropriately. HPES recommends maintaining updated inventories of all assets and data in a classifiable way and, within an infrastructure designed to protect that type of data

Ref#	Category	Question	Supplier Response
			from likely attack vectors (distributed denial-of-service [DDoS], theft, ransomware, etc.).
Q48.	Security	Do you have any guidelines or best practices regarding whether the various Managed Security Services are better off being remotely hosted or on premise?	Both solutions—if implemented correctly—can provide a high level of security awareness and interdiction within your environment. Remotely hosted (leveraged) solutions are significantly less expensive and, for most Managed Security Services, offer better protection than small dedicated (on-premise) solutions. Access to qualified and skilled resources at low cost is usually the top reason an organization will seek out a leverage Managed Security Solution. The next benefit is larger context, more visibility as a leveraged security operations center (SOC) sees many similar networks across the globe while an on-premise SOC typically sees only its own environment.
Q49.	Security	Do you think you would be able to provide all the described Managed Security Services yourselves or will you require to subcontract any services to other third parties?	HPES is capable of providing all listed Managed Security Services listed. From time to time we partner with Advanced Persistent Threat (APT) hunting/monitoring firms if necessary. Our procurement and sustainment strategy acknowledges the benefits of highly specialized firms with deep niche knowledge in the areas of APT hunting and monitoring. To accomplish this, we defer to these experts, who partner with us across a wide range of programs. For VITA, we will help to focus on the specific needs of the Commonwealth in this regard and provide the options and proven capabilities needed through our dedicated partnerships and portfolio of unique security firms to provide a range of services that can be tailored to match the needs of the VITA program and stakeholders.
Q50.	Scope Demarcation	VITA is interested in identifying the most efficient demarcation or bundling of these services between RFPs. For example, perhaps it would be more efficient to separate the Data Center facilities from the other Server services; or perhaps it would be better to include some or all of the Security services with the Server RFP. Please provide any further experience or suggestions regarding	HPES embraces the operational concept of an MSI environment however, the levels of service tower granularity in some deployments have introduced unnecessary and unmanageable levels of discontiguous service dependencies. There are natural operational service dependencies like those

Ref#	Category	Question	Supplier Response
		scope demarcation between potential RFPs.	referenced in VITA's question "facilities versus server versus security". The facilities operational status (HVAC metrics) used to house a server footprint (data center) are vital to the overall operational footprint of server service delivery and its associated service dependencies. For example, power outages, HVAC, UPS etc., are examples of server service dependencies from both Data Center and Server. Another use case involves physical and logical access controls (security) that may negatively impact server service delivery and/or server availability. Operational security related metrics either physical access controls (un/authorized data center server rack cabinets) and/or logical access controls (authentication based access) are a required security service dependency that contribute to the overall server dependencies and are correlated to give the overall server service availability. Security deviations/events can and typically do impact a server/s ability to provide an available end-to-end service. Should VITA choose to introduce this level of operational supplier granularity, each separation of supplier service would require additional supplier management activities/governance and suppliers systems management integration activities to "re-build" the dependencies needed to view holistic server service delivery given the operational sprawls across multiple suppliers. The added integration management (both supplier operational governance and suppliers system integration) required to both produce and operate in an MSI construct can be challenging and will require procurement experience and technical expertise to make certain that all aspects of the proposed VITA roadmap are adequately covered and that the demarcations created can fit together seamlessly into one centralized Managed Security Services platform.
D.	**Financial/Managed Security**		

Ref#	Category	Question	Supplier Response
Q51.	Pricing Structure	The Commonwealth is interested in creating the best possible pricing structure for the Services. In light of that fact, Supplier is invited to both comment on the structure described in Exhibit 4.1 and 4.2, and to propose an alternate pricing structure if they believe that it will better serve the interests of both parties. The Commonwealth will contemplate any proposed pricing structure along five dimensions: 1. **Predictable:** To the greatest extent possible, customers should be able to forecast charges ahead of time; changes in pricing that occur over time should not be a surprise. 2. **Manageable**: The pricing should not be so complex that it is needlessly difficult to administer. If quantities of work or equipment in the environment must be measured, then those quantities should be as easy and transparent as possible to measure. 3. **Fair:** The service pricing must be a reasonable proxy for a services provider's underlying costs and should adequately recover those costs. Additionally, to the extent possible, the party that causes any incremental cost should bear that cost. 4. **Incentives:** All pricing structures will incentivize certain behaviors and discourage others. The goals of the sourcing program must be kept in mind when considering the behaviors that might be driven by a pricing structure. For example, a goal to encourage server consolidation might include reduced cost at a centralized data center. 5. **Flexible:** As consumption moves up and down,	Pricing recommendations for security align to our response to Question 35 using a service catalog approach to meet the Commonwealth's dimensional pricing requirements. Once again, service tiers would be applied, as appropriate, for each security service offered. For Security Services, the COV has identified numerous discrete Resource Units (RUs) for security services. Though these are separately identifiable requirements, many are not separately tracked as discrete activities due to overlapping of resources. We recommend this list be collapsed with other RUs that have the same Unit of Measure, as defined in tab "3-Resource Baselines" (e.g., combine Desktop Encryption with Desktop Managed Host Intrusion). Collapsing this list will make it easier to manage while still flexible in offerings.

Ref#	Category	Question	Supplier Response
		the charges should also adjust. Technology is an evolving industry, and the ability to turn down an old service to turn up a new service is one of the benefits of an efficient IT sourcing agreement. Such adjustments may include minor volume changes month to month, significant scope additions, reductions, or terminations, and ability of large service providers to re-deploy investments.	
Q52.	Inventory and Volume Collection	The Commonwealth is interested in introducing new Resource Units that do not exist in the current contract; in order to fairly compensate Supplier for service delivered, and support the other goals described in question 36, Supplier is asked to describe their experience and approach to collecting and verifying volumes both before and after contract signing, and the approaches they use to adjusting financials in the event that the initial count is incorrect. For example, today database support is provided by the Supplier, but is not separately billable. The Commonwealth sees an advantage to separating out database support and making it a separate chargeable unit, how would the service provider collect and verify the volumes to support this chargeable unit?	We describe our asset management and baselining process in our answer to Question 36.
Q53.	Asset Ownership	The Commonwealth consumes certain services today which are underpinned by a set of assets (servers, firewalls, etc.). The Commonwealth (or their designee) has the right to acquire these assets. The Commonwealth has a desire to consume services; rather than own assets, and envisions Supplier acquiring these assets and using them to provide services back to the commonwealth. Please describe experiences acquiring assets from an incumbent, and also describe your recommend financial treatment of their cost recovery for these assets.	HPES has access to, and close working relationship with, HP Enterprise Financial Services (HPEFS). HPEFS is able to buy legacy assets and lease them back to HPES. HPEFS would perform a valuation of the legacy assets and provide the resulting lease cost, which would then be included in the monthly RU service price offered by HPES.

6. FEEDBACK REGARDING RFI DOCUMENTS

Please use the table below to provide commentary regarding specific documents included within this RFI, adding rows as necessary.

Ref#	Document/Section	Supplier Commentary
C1.	Exhibit 02.1-a Exh (Description of Services - Server-Storage-Data Center LAN), 4.2.2.3 New COV Private Cloud R595: 7. Provide sufficient capacity to handle VITA and VITA Customer's elasticity requirements.	To make private clouds an affordable option for enterprises, the capacity of the environment needs to be effectively defined and managed. Too small an environment deprives the enterprise of the flexibility and elasticity it is seeking in a cloud service, and too large an environment will lead to unused capacity and higher costs. VITA should provide additional details on its expectations regarding the initial capacity requirements of the private cloud that bidders can use to properly size and price the service.
C2.	Exhibit 02.1-a Exh (Description of Services - Server-Storage-Data Center LAN), 2.3 Operations, Maintenance and Monitoring	Are the current tools in place owned by the Commonwealth, and would they be made available to the supplier. If yes, please provide a list of the tools.
C3.	Exhibit 02.1-a Exh (Description of Services - Server-Storage-Data Center LAN), 2.3 Operations, Maintenance and Monitoring R82: 8. Manage, maintain, monitor, and control online and batch processes, both scheduled and unscheduled (including on-request processing).	What are you currently using to manage the batch processing capability? Please provide a list of the number of batch jobs per day that are processed.
C4.	Exhibit 02.1-a Exh (Description of Services - Server-Storage-Data Center LAN), 2.3 Operations, Maintenance and Monitoring R89: 15. Monitor, verify, and make appropriate adjustments to support proper Applications executions.	Clarify if this statement is in reference to tuning the HW environment in support of the application owners.

Ref#	Document/Section	Supplier Commentary
C5.	Exhibit 02.1-a Exh (Description of Services - Server-Storage-Data Center LAN), 2.3 Operations, Maintenance and Monitoring R95: 21. Provide remote monitoring and management of Servers, storage Equipment, and associated peripherals not located at the Supplier-operated Data Center as indicated in Exhibit 4.6 (Equipment Assets).	Will the Commonwealth provide smart-hands support at each location?
C6.	Exhibit 02.1-a Exh (Description of Services - Server-Storage-Data Center LAN), 4.1 Common Platform Services R432: 11. Build Application packages, based on customer requirements, for deployment.	Can you provide historical data on how many applications packages are created for deployment per month?
C7.	Exhibit 02.1-a Exh (Description of Services - Server-Storage-Data Center LAN), 4.6.2 Middleware Services	Please provide a list of middleware in use and the number of instances.
C8.	Exhibit 02.1-a Exh (Description of Services - Server-Storage-Data Center LAN), 3.2.2.1 Enclave	Can the Commonwealth provide additional information about the enclaves? Can they be logical or physical?
C9.	Exhibit 02.1-a Exh (Description of Services - Server-Storage-Data Center LAN), 7.5.4 Remote User VPN (clientless) R1159: 1. Provide secure remote access, including clientless access to authorized web Applications,	Can the Commonwealth elaborate on the extent of voice services, VoIP services, and VTC services support under this contract?

Ref#	Document/Section	Supplier Commentary
	client/server Applications, Voice, and file sharing to VITA and VITA Customers, and designated Third Party Vendors	
C10.	04.1-a Exh (Server, Storage and Data Center Pricing and Volumes Matrix) - Tab 1-Baseline Charges	Please note that the subtotal from "Data Center Services" (row 87) is not included in the sum for the Total Charges in row 100.
C11.	04.1-a Exh (Server, Storage and Data Center Pricing and Volumes Matrix) - Tab 2-ARC RRC	Tab 2 defines the unit of measure for firewall services in terms of price per GB of traffic inspected. This does not appear to be an effective chargeback mechanism. We are not certain that we would be able to ascertain which traffic belongs with which customer at a reporting level. In addition, the cost for service provided is driven by the firewall instances, not by the traffic actually inspected. Each firewall will have a traffic capacity limit—and as such, should be calculated based on the number and types of firewalls, which is a truer indication of the cost for that service, and then allocated to customers based on the number of instances that they have ordered.
C12.	04.1-a Exh (Server, Storage and Data Center Pricing and Volumes Matrix) Multiple tabs	It appears as though VITA anticipates different types of Disaster Recovery (DR) services, which is what we would also recommend. DR is not simply a flat uplift charge, but varies by service type based on complexity and system. Since the total charges for this service are included in the total evaluated price, for ease of evaluation our recommendation is that VITA define the services and associated volumes.
C13.	04.1-a Exh (Server, Storage and Data Center Pricing and Volumes Matrix) Tab 11- True-up Allowances	We request an additional description of the Tab "11- True-up Allowances." It is unclear how this tab should be populated and how it will be used in contract execution.
C14.	04.1-b Exh (Pricing and Volumes Matrix - Managed Security) Tab 3-Resource Baselines	Please clarify the difference between rows 9 and 10 and row 24. Rows 9 and 10 are FTE units of measure, but row 24 is a pool of FTEs—whereas rows 9 and 10 are not. What is the difference in how these RUs would be ordered?