Unisys Response to Commonwealth of Virginia

Virginia Information Technologies Agency (VITA) Supply Chain Management Division

Request for Information (RFI) 2017-14 For Server, Data Center, and Security Services

Original

Unisys Corporation
801 Lakeview Drive, Suite 100
Blue Bell, Pennsylvania 19422

UNISYS

Tony West
Account Executive
Public Sector Industry

Unisys Corporation
801 Lakeview Drive
Suite 100
Blue Bell, PA 19422

Telephone
(770) 335-3725

UNISYS

October 21, 2016

Greg Scearce
Commonwealth of Virginia
Virginia Information Technologies Agency (VITA)
Supply Chain Management Division
11751 Meadowville Lane
Chester, VA 23836

RE: Unisys Response to Virginia Information Technologies Agency (VITA) RFI 2017-14 for Server, Data Center, and Security Services

Dear Mr. Scearce,

Unisys understands the important role the Server, Data Center and Security Services RFI will play in achieving your vision to implement a new IT Infrastructure Services program. As a long standing partner to the Commonwealth of Virginia, we are pleased to participate in your efforts to deliver agility, speed, and balance between individual agencies and the enterprise.

We acknowledge your overarching intent for this RFI is to gather current market insight to determine the scope and improve the quality of the resulting RFP(s). To help achieve this end, we assembled a multi-disciplinary team knowledgeable in both public and private sectors as well as experienced in VITA to prepare our response. While specific recommendations are documented within, our summary advice is the Commonwealth releases two RFPs, one for Server, Storage and Data Center and the other for Managed Security Services:

- Cloud, server, storage, backup, network, and disaster recovery services should be provided through a single program to maintain the quality of service, integration between technical platforms, and support the planned transformation into private and public cloud hosted environments.

- Security services should be separated into its own tower to maintain the risk management, security governance, and regulatory audit requirements needed without compromise to operational needs.

Thank you for this opportunity to contribute to this RFI. Should you have any questions, please contact me at 770-335-3725 if I can be of further assistance.

Sincerely,

Tony West
Account Executive
Unisys Public Sector

TABLE OF CONTENTS

Respondent Contact Information 1
Questions 2
A. Server Storage Services 2
B. Financial/Server Storage 19
C. Managed Security 22
D. Financial/Managed Security 29
Feedback Regarding RFI Documents 35

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	Unisys Corporation
Company Mailing Address	801 Lakeview Drive, Suite 100 Blue Bell, PA 19422
Company Website Address	Unisys.com
Name of Contact Person	Tony West
Contact Person E-mail Address	Tony.West@Unisys.com
Contact Person Telephone #	(770) 335-3725

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?	Unisys provides our response as follows.

Unisys Response:

In order to establish a strong foundation for IT operations and service availability, manage the transition period, and provide cost effective services for the Commonwealth of Virginia agencies and users, Unisys uses many best practices to operate services in centralized and non-centralized data centers. The following best practices are highlighted to support the non-centralized data centers and provide quality and consistent services.

- Develop a Services Management Manual (SMM) – This documentation and shared knowledge base will provide the common processes and unique details to be used to manage the Commonwealth's IT services to the defined Service Level Agreements (SLAs) and centralize individual agencies' specific operational requirements and tasks. This manual also will become part of the basis to identify areas for improvements and opportunities to transform individual data center services into repeatable practices.
- Provide at least two centralized locations for vendor tools and operational support. Centralizing vendor operations will improve the timeline for implementing service, maintain continuity of services, manage costs, and improve security by limiting the access points from the vendor into the Commonwealth of Virginia environment.
- Establish the security framework early and apply during the transition period. Many agencies are required to meet multiple Federal regulations. To satisfy each agency's concerns and support audit readiness, a security assessment and a security manual should be completed early in the transition period. This will enable the agencies to communicate with their security organizations and regulators consistently and provide a reportable metric for maintaining the security controls of the environments.
- Use centralized data protection in order to back up systems in the non-centralized data centers. The centralized backups also provide additional options to support business continuity needs and migration to the centralized data centers or the cloud.

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.	Unisys provides our response as follows

Unisys Response:

Unisys believes that the public sector is well served by 3 to 4-year contracts with optional annual extensions totaling 8 years, especially when they include financial targets for service cost reductions.

This contract length provides an appropriate time cycle to transition the services, stabilize and improve IT operations, and prepare for transformation to the next generation of technologies and services. Additionally, the contract length can reduce cost and resources required by the Commonwealth for developing and processing new procurement proposals.

Longer contract lengths can limit the ability to refresh technologies and migrate to services that meet changing business requirements due to user order commitments and can shift the focus on daily operations over innovation.

Q3.	Data Center	What do you recommend for the length of the contract for the Data Center Facility for this type of environment?	Response below.

Unisys Response:

Unisys recommends vendor-managed Data Center Facility contracts aligned with the contract period and transformation strategy related to question 2.

Because the Commonwealth of Virginia includes several non-centralized data centers, the transition period, continued use and potential consolidation for each data center should be taken into account and the associated length of the support should be defined separately within the contract.

Q4.	Server/Storage	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?	Unisys provides our response as follows.

Unisys Response:

Unisys recommends a 3-year average technology refresh cycle for Server and Storage Systems. Unisys also recommends a 5-year average technology refresh for Network Infrastructure. The actual refresh plan depends on various factors, including reusability, technology shifts, vendor support cost, and end-of-service life status. The technology refresh rate does not affect the length of the contract, but it can affect the pricing of the technology and related services.

Q5.	Server/Storage	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 in the Server RU structure?	Unisys provides our response as follows.

Unisys Response:

When using a separate hardware charge, Unisys recommends Resource Unit (RU) pricing, which includes the hardware cost and annual maintenance during the initial deployment period (typically 3 years) and then reduces to include only the annual maintenance costs until the service order is discontinued. Technology refreshes typically require a migration to a new service, which will reset the hardware charge.

Unisys also recommends moving toward a consumptive Opex model for the hardware. Several technology vendors provide options that provide access to a consistent service price and remove the need to emulate the hardware charges, especially for private cloud or virtual hosting environments.

Q6.	Server/Storage	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?	Unisys provides our response as follows.

Unisys Response:

Unisys provides Server, Mainframe, and Compute Services solutions in a tiered structure as described in the provided Exhibit 3.2.

Server service tiers based on availability must take into account details on the facility, technology, and requested functionality. Services designed up to 99.9 percent availability present few challenges unless the site cannot support that level of availability. Services requiring higher levels of availability require additional considerations that require technology or support that may not be identified in an RFP or multiple instances in the environment.

Capabilities for multiple tiers in storage are shifting rapidly. To provide the best options for storage tiers, adequate volume within each tier is critical to receive the best price. Functions, such as replication and data deduplication, are also key aspects to consider including in specific service tiers.

Unisys has extensive experience with operating and managing in a tiered service model for complex, mixed computing environments worldwide, including the Commonwealth of Pennsylvania and California State University.

One recommendation is to add a Basic service for servers that will provide the Commonwealth's users with a lower cost alternative that has fewer operational restrictions such as reboots and performance monitoring for development and quality assurance platforms. As the Commonwealth moves toward a Hybrid Cloud and As-A-Service solution, this tiering approach can also be applied with equivalent configuration requirements.

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?	Unisys provides our response as follows.

Unisys Response:

Unisys recommends establishing a distinct catalog of services and RUs that Commonwealth of Virginia users will use and a second catalog for the vendor's components and underlying services. The first catalog will support maintaining a simplified catalog of specific services that the Commonwealth would order. The second catalog will provide the underlying services that can be combined and used to create the services presented in the service catalog. The second catalog will also enable options to present new services to the Commonwealth while reusing the various service components.

As cloud offerings and new technologies are incorporated into the Commonwealth, this model will reduce the complexity presented to the users and encourage use of the services.

Unisys also recommends limiting the size of the catalog for certain services, such as Server and Storage, by standardizing the configurations of servers (such as using small, medium and large sizes) and the types of storage (based on performance and access methods).

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 Commonwealth?	Unisys provides our response as follows.

Unisys Response:

Based on the tiered Service Levels, Unisys would provide the Commonwealth with a tiered approach to the services. Platinum Services require three or more data centers setup to support active-active-active failover functionality, clustering, load balancing, and data replication. For Gold (99.99 percent) support, we recommend using two data centers to provide an active-active solution that use redundant components with automatic failover. For Silver (99.9 percent) support, Unisys recommends using one data center for production with clustering and load balancing. For Bronze (99.4 percent) and Basic support, a single data center is sufficient, and server clustering is optional.

Unisys recommends evaluating disaster recovery requirements and services independently from the production service tiers. Gold and Platinum service tiers can use the Disaster Recovery (DR) data center to provide business continuity support.

To best use the multiple data center capabilities for the Platinum and Gold service tiers, Unisys recommends that the Commonwealth evaluate its applications and create transformation plans to adjust the application architecture to use the multisite functionality.

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?	Unisys provides our response as follows.

Unisys Response:

Based on Commonwealth's approach of using a MSI supporting the service integration and management, including governance; and integrated service towers, Unisys recommends maintaining the following RFP and service structure.

- Data Center Hosting Services - The cloud, server, storage, backup, network, and disaster recovery services should be provided through a single program to maintain the quality of service, integration between technical platforms, and support the planned transformation into private and public cloud hosted environments. Using this structure will also enable the Commonwealth to benefit from additional disruptions in the technology marketplace and the continued transformation to a Software Defined Enterprise.
- Managed Security Services – In order to provide a strong foundation and enable a common framework for protecting the Commonwealth's systems, application and data in the cloud and in the on premise data centers, Unisys recommends separating security services into a separate tower. This structure will also support maintaining the risk management and security governance required to enable the agencies to meet their desired outcomes and regulatory audit requirements.

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?	Unisys provides our response as follows.

Unisys Response:

Unisys recommends evaluating additional storage options based on business requirements. Object-based storage is a key storage service in cloud environments and can be considered an alternative to file services and unstructured data storage. If the Commonwealth has a large amount of unstructured content, we recommend object-based storage to improve management, reusability, and control of the data.

Unisys also recommends predictive and virtualized storage as a standard. The use of storage virtualization provides capabilities to improve the availability of the storage services and enable performance controls in the storage environment.

Unisys offers object-based storage and virtual storage based on the gigabytes of storage consumed in either type of storage and allocated or used volume. In a highly virtualized storage environment, using thin provisioning and performance-based assignments, Unisys recommends transforming from allocated to used charges for a more accurate and cost-effective view of the storage consumed.

Q11.	Server/Storage	The Commonwealth is interested in ensuring it provides optimal	Unisys provides our response as follows.

		storage performance and availability for VITA and VITA's Customers. How do you propose to provide and measure this performance?	

Unisys Response:

Unisys best practices for storage services use storage virtualization to establish, maintain, and monitor the performance of the service tiers in the storage environment for each server.

Unisys measures the storage performance based on the input/output operations per second (IOPS) assigned to the individual physical servers.

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.	Unisys provides our response as follows.

Unisys Response:

Unisys recommends using a cloud management platform that can provision and manage server instances in the existing virtual hosting environments and a private cloud. Using a cloud management platform provides the ability to assign workloads based on policies and supports transitioning workloads as environments are transformed and refreshed.

Virtual server environments can be transformed to provide the same capabilities and functions as those of a private cloud. We recommend evaluating each environment to determine if it is appropriate to upgrade the functionality or transform with a new implementation.

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)?	Unisys provides our response as follows.

Unisys Response:

Considering the Commonwealth's vision of "delivering agile technology services at the speed of business," Database as a Service (DBaaS) can deliver value to the enterprise in different ways:

Unisys recommends considering DBaaS as part of DevOps initiatives and automation. By providing the capability to support DevOps and Agile Development Methodologies, DBaaS provides the foundation for quick provisioning while maintaining the required levels of standardization, reliability, security, and quality of services.

With predefined and advertised costs, each agency will be able to use the right services for its requirements, knowing exactly how much that will cost it.

Additionally, centralized IT will be able to charge back the correct costs, based on the agency's utilization, to allocate the costs accurately.

With a simplified, consolidated, and standardized database environment, the Commonwealth can optimize the costs of licenses, hardware, and labor as well as simplify support of the environment.

Unisys recommends providing enhanced database services for physical database administration (DBA) (managing and maintaining the database software), logical DBA (supporting the database structure and data), and database development. These services can be provided on a per database instance or a time and materials basis.

Unisys also recommends using a Database Firewall Security service to protect the Commonwealth's data.

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?	Unisys provides our response as follows.

Unisys Response:

As referenced throughout the RFI, the key cost and value service drivers are tied to the definition and acquisition of the required server configurations and infrastructure combinations that are required.

Additionally, Unisys recommends developing services that are reusable and standardized. Highly customized services to meet unique and low-volume activities will drive costs higher and be difficult to extend to support new requirements.

Although not referenced in the provided documentation, the infrastructure requirements to support very high availability requirements, such as 99.999 percent, tend to be cost prohibitive. Although Unisys supports this option on many client deals, they are rarely implemented because of the delivery cost and the necessary modifications in the client's applications.

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?	Unisys provides our response as follows.

Unisys Response:

Unisys recommends that the Commonwealth define the planned uses of the Enterprise Key Management service. They can include Identity and Access Management (IAM), including integration with Active Directory and other identity management systems; databases; encryption, such as Secure Socket Layer (SSL); tokenization; and development, including code signing. This information will support designing and providing the appropriate solutions to meet the Commonwealth's business needs and service requirements.

Because the key management system is a core function in an enterprise, Unisys advises that key management should be included in the IAM scope. This supports the integration of key management Active Directory (AD) and other identity management services, access control, and configuration to support self-service for creating other certificates and keys.

Unisys also recommends reviewing the SANS Institute's white paper on the best practices for evaluating and creating an encryption RFP. SANS is a recognized leader in security training and practices. The white paper is available at the following link: https://www.sans.org/reading-room/whitepapers/analyst/encryption-procurement-setting-standard-34655.

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?	Unisys provides our response as follows.

Unisys Response:

Unisys recommends using a centralized automation system to integrate the various IAM services in order to enable Commonwealth users to request IAM activity once and receive consistent service. After the services are transitioned to Unisys, we recommend reviewing the IAM services and technologies to identify overlaps which can impact the users and applications. Unisys recommends developing a transformation roadmap to develop a plan to provide enterprise IAM services.

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?	Unisys provides our response as follows.

Unisys Response:

Unisys agrees with the overall structure and handoffs between the Commonwealth, the MSI, and the support organizations. By using ITIL v3 as the common service management and governance framework, the Commonwealth will gain consistency and reliability using the defined processes.

Unisys has worked with MSIs; we are working with an MSI for a large state government contract.

Unisys has the following recommendations for MSI's interaction with suppliers:

- Treat suppliers as partners and not vendors
- Foster trust between VITA and suppliers
- Foster trust among suppliers
- Define responsibilities clearly on a Joint Responsibility Matrix
- Establish SLAs that directly support the Commonwealth's business needs
- Establish a service provider council early to give larger service providers (versus MSI only) input to the Commonwealth's strategic direction
- Develop governance processes that address single occurrences of service provider underperformance in IT processes with shared SLAs
- Avoid service providers that underbid their scope of work.

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)?	Unisys provides our response as follows.

Unisys Response:

Unisys does not recommend that the facility provider provide common operating monitoring groups. As the Commonwealth transforms to include cloud and Software as-a-Service (SaaS) services, data center facility management will have limited to no interaction with the day-to-day operations of those services.

Unisys recommends establishing a common Service Integration and Management (SIAM) platform for automating IT service management (ITSM) functions based on alerts from monitoring services.

By providing the common SIAM, the Commonwealth's service providers can bring the appropriate tools to the environment and adjust the tools as technology is added or changed.

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, development, operations, testing, and coordination. What role should VITA's MSI should play in this effort in relation with the Server Services provider?	Unisys provides our response as follows.

Unisys Response:

VITA's MSI should oversee development and management of Business Continuity and Disaster Recovery governance, each specific to a single agency or even applications. As part of this governance, the MSI should specify the SLAs, such as Recovery Time Objective (RTO), Recovery Point Objective (RPO), and Account Owner (AO) This will help the Server Services provider to design the appropriate DR solution. Additionally, the MSI should coordinate the execution of a periodic DR test to ensure that the DR solution performs according to the VITA's requirements.

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?	Unisys provides our response as follows.

Unisys Response:

For Disaster Recovery, Unisys recommends using at least two centralized data centers. The two data centers should be located more than 150 miles apart or be geographically separated to provide protection from regional disasters.

Clients have also begun to use multisite availability. Unisys recommends using two data centers less than 50 miles apart to support active-active high availability and synchronous data replication. This provides protection from a single data center fault but will not provide protection for a regional disaster.

If Commonwealth applications require high availability with business continuity, Unisys recommends linking the multisite data centers with a DR environment to provide protection against a regional disaster.

As the Commonwealth continues the transformation to include cloud services, Unisys recommends evaluating applications that can use cloud as part of the multisite High Availability and DR environments.

As the Commonwealth considers High-Availability hosting options, the application's architecture must be taken into account. Although many applications are designed and developed to support load balancing and clustering, some applications will require modifications to best use multisite and cloud services.

Although multisite data centers provide improved application availability, the number of sites can dramatically affect the Commonwealth's costs and reduce options for maximizing the scale.

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?	Unisys provides our response as follows.

Unisys Response:

Unisys recommends separating Transition and Transformation projects and activities. Transition includes the program management for Unisys to assume responsibility and support for existing environments. Transformation provides support for migrations and introducing new technologies and service offerings. Migrations to new service offerings should include the following activities:

- Gather data and analyze it to develop the overall plan
- Build a Master Migration Plan
- Create site readiness and implement the target environment
- Perform a validation test before performing a migration
- Execute the migration plan
- Receive acceptance of complete migration.

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?	Unisys provides our response as follows.

Unisys Response:

In addition to the enhanced services that the Commonwealth identified, Unisys recommends Application Programming Interface (API)/Web Integration Services as a Service. API services provide a common platform to enable secure data interaction and transformation between multiple applications. This service would be delivered as an enterprise service that can be shared by many agencies.

As application and business service availability becomes the focus of Commonwealth operations, Unisys recommends providing Application Performance Monitoring. This advanced monitoring service provides information on how an application is behaving and can identify incidents and faults based on transaction volumes and delays that infrastructure monitoring services cannot identify.

Unisys also recommends considering Unified Communications as a Service and Workspace Productivity as a Service. As the Commonwealth's users continue to increase access to information regardless of where they are and which device they are using and the Commonwealth continues to integrate cloud services, adding Unified Communications and Workspace services will enable flexibility to provide end users with a common point of interaction for instant messaging and phone services as well as provide secure access to information, including "follow-me" data interaction.

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?	Unisys provides our response as follows.

Unisys Response:

Unisys recommends evaluating services to provide DevOps technologies, enterprise portfolio management, and cloud data archival services. These services provide advanced capabilities to improve application management and data protection.

Q24.	Enhanced Services	What would you propose as a good business case for virtualizing the desktop (offering VDI)?	Unisys provides our response as follows.

Unisys Response:

Unisys believes the best business cases for VDI is the prevalence of Bring Your Own Device (BYOD) and increasing regulatory security controls. Workspace productivity services such as VDI provide capabilities to supply common services across multiple platforms and reduce the potential for data to be exposed because of a lost or stolen device.

As millennials increase in the Commonwealth's workforce, the demand for VDI will increase. Millennials are very comfortable working with mobile devices and look to use productive services with the technology that best fits their needs. Enabling VDI will provide options that support the use of different user platforms while maintaining access to the Commonwealth's critical applications and providing data security.

Workspace services are delivered in a per-user/per-month subscription pricing model that maps specific services to defined user communities, such as customer service representatives, managers and VIPs. This reduces the capital expenditure required for application and infrastructure upgrades and provides ongoing flexibility of IT costs.

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.	Unisys provides our response as follows.

Unisys Response:

Unisys recommends using the WAN routers, or external aggregators, for the data center facility as the best demarcation point to separate the data center LAN from the facility network and WAN services. For the noncentralized data centers, the facility firewall or distribution router in the facility may be more appropriate, depending on the current network architecture.

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?	Unisys provides our response as follows.

Unisys Response:

Unisys strongly agrees with this approach because one vendor will perform troubleshooting across the entire data center. As integrated solutions include LAN infrastructure and Software Defined services virtualize the network functions, the network hardware management shifts to software configuration.

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?	Unisys provides our response as follows.

Unisys Response:

Unisys believes that the Commonwealth's approach is correct. However, we recommend implementing a Data Center Infrastructure Management (DCIM) solution and linking the DCIM to the rest of the data center (server, storage, network, etc.) management. This will help in optimizing power and cooling across the racks and using this information in optimal placement of virtual machines.

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?	Unisys provides our response as follows.

Unisys Response:

Unisys agrees with this approach; we adopted this approach in our own data centers.

To maintain a green data center, this process minimizes or eliminates stranded assets or commonly known as zombie servers. Having an owner for each device, and charging each month for power and space, ensures that the owner will consider the use of that device in addition to maintenance costs, network ports, and storage allocations.

Unisys charges each client account for the use of the data center facility. However, these charges are typically not shared with the client on a managed services contract.

Colocation clients are well aware of their facility costs because this is typically a unique element of their contract for using the data center. Many colocation contracts have a variable power rate that motivates the client to minimize the equipment in service.

As the Commonwealth continues transforming to increase virtualization and private cloud services, the direct visibility of the data center facility costs will decrease. In these environments, there is no one-to-one relationship between the physical hardware and the systems that the Commonwealth agency deploys.

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?	Unisys provides our response as follows.

Unisys Response:

Unisys recommends that LAN services be included in the same procurement or added to the existing vendor's contract as the noncentralized data centers are brought in as part of the scope.

As the noncentralized data centers are incorporated into the services, maintaining data center LAN services will support providing common capabilities and automation in the centralized and noncentralized environments. This will also provide improved options to migrate the noncentralized network environment to a central data center.

The tradeoff can be that some of the noncentralized data center LAN infrastructure may be used for the facilities other functions. If so, additional activity may be required to transform the environment to separate the data center from the rest of the facility network. This activity may require additional investment for the Commonwealth and planned outages.

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?	Unisys provides our response as follows.

Unisys Response:

Unisys recommends that the provisioning and management of data center-to-data center connectivity should be managed by the same provider as that for the data center hosting services (server, storage, and network).

Data Center to Data Center communication is critical to interaction to support multi-site hosting, data replication and load balancing between the data centers. As such, this connectivity is typically tied to the services and their operations. As a result, it is recommended to maintain them separately from the Commonwealth's network and system access.

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?	Unisys provides our response as follows.

Unisys Response:

Unisys proposes a phased and comprehensive approach to assess and implement the CESC data center migration. This approach focuses on several key areas. First, we will identify risk and risk mitigation. To maintain a seamless migration, Unisys treats these moves like a controlled disaster recovery—every action is planned, tested, and validated with documented, rehearsed backout and contingency plans. Second, in our business- and application-centric approach, we will take the time to detail business requirements and understand application interdependencies' disruption to the business. Finally, we will use a thorough and comprehensive program management methodology to make the data center migration as smooth and undisruptive as possible and not shortcut planning activities.

Phase 1, Data Gathering and Analysis, will concentrate on developing a complete understanding of the current application and infrastructure inventory. Using this information, Unisys will be able to identify the requirements that will be used as input to the overall migration plan. A master migration plan will be negotiated with business stakeholders to minimize potential impacts on normal business operations while achieving the June 2019 date. Phase 1 will concentrate on the following key areas:

- Project and resource planning
- Application inventory and physical asset inventory
- System and application mapping, including dependencies and interdependencies
- Identifying assets or applications that will be retired, moved, or consolidated
- Identifying requirements such as outage windows, change control process, validation needs, site availability, and capacity constraints
- Aligning the applications and systems with move groups or migration bundles
  - Selection of migration strategies and technical requirements for each application that are based on application RTO and RPO
  - Physical moves and data migrations to new "seed" equipment at the target site are two examples of migration strategies
- Rationalizing the server configurations, including deciding whether to virtualize or adjust the specifications
- Mapping to the appropriate destination cloud or data center
- Building a Master Migration Schedule.

The overall goals of Phase 1 are to discover the assets to be moved and agree upon a migration schedule.

Phase 2 will be the detailed site planning that establishes target site readiness to host the moved assets. Design of the new storage assets, verification of network and facilities plans, and a rollout plan for new assets will be completed at this time. This phase includes the following key goals:

- Validate that target site buildout plans will meet the time and infrastructure needs for the asset migration
- Validate that new storage infrastructure is designed appropriately and in order

- Validate that new server rollouts are timed appropriately to meet the migration schedule
- Finalize scheduling for transportation and Original Equipment Manufacturer (OEM) recertification of assets.

At the conclusion of Phase 2, Unisys and the Commonwealth will agree to initiate migration activities.

Phase 3 will be the execution of the move plans. For each move group, Unisys will create detailed task-level run books that choreograph every action during the move. These plans will be tested in tabletop exercises; the actual moves will be coordinated by Unisys and tested by the application support teams. This phase includes the following key activities:

- Finalizing detailed night-of-move project plans
- Completing migration workbooks containing detailed procedures for application shutdown, server power-off/power-on, and other key technical activities
- Testing and rehearsal of move activities
- Final site visits to confirm that the target site is ready for asset move
- Disassembling, packaging, transporting, and reassembling assets
- Verifying proper functionality at the target site.

Phase 3 will conclude with the Commonwealth's acceptance of the Data Center migration.

The Unisys Data Center migration methodology was successful in dozens of large data center moves. Key to our success is a disciplined quality assurance (QA) program. Unisys will assign a Subject Matter Expert (SME) who is not directly involved on the engagement to review the project at predetermined points known as QA gates. The QA reviewer will look for issues that create risk in several areas with an emphasis on those that may jeopardize the migration timelines or pose a threat to maintaining normal business operations. The QA reviewer will meet with a set of the Commonwealth's stakeholders and project sponsors to review how well Unisys is meeting expectations.

Unisys recommends using like-for-like migrations to provide expedient migrations. We consider like-for-like to be based on maintaining a common platform (such as a window server) rather than focusing on a specific specification. Some applications and business initiatives may be a good fit for migrating to new services. We also recommend additional planning and testing when using new services to avoid affecting the Commonwealth's operations.

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?	Unisys provides our response as follows.

Unisys Response:

Unisys will implement a Hybrid IT model that will allow the Commonwealth to take advantage of new, cost-efficient services in the public cloud while making appropriate choices on how to leverage investments in infrastructure and private clouds.

The Unisys Cloud Management Platform is a key component that enables modern Hybrid Cloud Managed Services and is a flexible and extensible foundation for operating a Software Defined Enterprise (SDE), including Infrastructure as Code (IAC) blueprints for client environments retained as client resources and automated deployment and management of infrastructure and applications from those blueprints.

The Unisys Service Management suite provides the same capabilities across the traditional data center and Hybrid Cloud environments, maintaining a consistent approach and level of service.

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?	Unisys provides our response as follows.

Unisys Response:

Unisys recommends that the Commonwealth own the cloud contracts and assign Unisys as the agent. This will enable the Commonwealth to use government contract pricing that is available only from the cloud vendor or through the GSA procurement process.

Unisys also provides cloud services as a reseller.

Unisys recommends using a cloud management platform that reports on usage and imports the pricing that the Commonwealth has for the cloud services. These reports provide the detail that the Commonwealth will need to show which agencies are using cloud services.

Q34.	Cloud Services	When the Commonwealth buys cloud services offerings how do you propose to identify where the data and services are located?	Unisys provides our response as follows.

Unisys Response:

Unisys recommends using a cloud management platform to manage the provisioning and use of cloud services. These platforms can track which service and hosting environment has the services and data. Additionally, we recommend developing a cloud strategy that will identify the cloud environments to be used for specific data, applications, and regulations. This information can be included in the cloud management policies to maintain the appropriate controls.

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. 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	Unisys provides our response as follows.

		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.	

Unisys Response:

Unisys is familiar with and amenable to the proposed pricing structure, but from an administrative perspective, we recommend a discussion focused on consolidating several of the data points (RUs). Additionally, Unisys recommends modifying the pricing sheets to separate assets and capital from services. This would allow the Commonwealth to effectively manage the asset and services utilization as required.

This pricing structure will well serve an on-demand consumption-based approach that cloud computing offers.

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 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?	Unisys provides our response as follows.

Unisys Response:

For items that are broken out into an RU structure, consistent with your Additional Resource Charge/Reduced Resource Credit (ARC/RRC) tables, Unisys recommends truing up monthly or quarterly, which will ensure that the Commonwealth will be billed only for actual use.

Although Unisys is receptive to increased transparency, we want to avoid the potential administrative costs of reporting and billing on sub-RU elements.

Unisys developed a proven methodology to collect and verify volumes before and after contract signing. This includes adjustments or true-ups to the financials if the initial count is incorrect. The following list shows the methodology used before and after the signing of the contract:

- Kickoff, Business Objective, and Schedule
- Applications, Infrastructure, and Process Discovery
- Application and Data Analysis, and Reports

- Workshops to Finalize Service Catalog and Volumes
- Development or updating of the cost model.

Unisys will use several automated discovery tools to discover the applications, database instances, virtual and physical servers, various tiers of storage, and network devices in the VITA IT infrastructure. We will conduct workshops with the appropriate stakeholders to fill gaps in the collected data. Using the final data, we will jointly work with VITA to define the chargeable units that will form the services catalog. Unisys can update the Configuration Management Database (CMDB) with the RUs defined and agreed.

For example, Unisys will define different RUs for database instance–based different Relational Database Management System (RDBMS) technology. Similarly, we will define the RUs for supporting these database instances.

Additionally, VITA can introduce new RUs such as Web Server Instance, WebSphere MQ (Processor Value Unit), BizTalk Server Enterprise (Processor Value Unit), Server Management Services, and Middleware Management Services.

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.	Unisys provides our response as follows.

Unisys Response:

Unisys has considerable experience with managing, acquiring, and procuring assets for our clients. Because the Commonwealth does not wish to own its assets and some assets owned by the incumbent may have useful life, we recommend a flexible arrangement by partnering with the vendor of the assets or a third-party financial partner to limit capital exposure to the Commonwealth and minimize ongoing expenses. The cost recovery for these assets would be built into the base charges or milestones. Unisys looks forward to a detailed discussion on asset ownership.

An approach that Unisys recommends is that VITA adopt a hybrid cloud model that allows it to move toward a consumption model. The migration to public clouds can be closely tied to tech refresh (instead of procuring new hardware, VITA can migrate the application or workload to public clouds and allow Unisys to manage these for VITA). Unisys offers the hybrid cloud operations and management service based on our Cloud Management Platform (CMP). As part of this offering, Unisys provides P*Q pricing, where P is the RU and Q is the monthly charge. Unisys has partnerships with Amazon Web Services and Azure and offers the service by using these public cloud providers.

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?	Unisys provides our response as follows.

Unisys Response:

Unisys understands the scope to include the elements found in the following RFI sections:

- 2.0, Security Services Overview
- 3.0, Information Security Program Requirements
- 4.0, Security Requirements.

We do not see challenges or issues with this bundled model.

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?	Unisys provides our response as follows.

Unisys Response:

Unisys recommends that the Commonwealth develop a plan and strategy for the development of a Managed Security Services (MSS) Center of Excellence (CoE). The CoE will enable the Commonwealth to deliver predictable, repeatable, consistent, and cost-effective MSS to its various agencies and constituents.

Unisys has the knowledge and experience, specifically in the public sector, to deliver an MSS CoE to the Commonwealth.

Although there are concerns to consider, Unisys proposes a methodology consisting of the following key categories:

- Overall IT security architecture
- Passive defense mechanisms
- Active defense mechanisms
- Ability to gather threat intelligence
- Offensive strategy.

Additionally, the interdependencies, nuances, and pain points between the categories will reveal the maturity of the Commonwealth's IT security framework.

From this baseline, we will work collectively with the Commonwealth's CIO and CISO as well as with VITA and ITAC on a growth and scaling strategy.

Q40.	Security	Can you provide examples of comparable environments where you offer security services similar to those required by the Commonwealth?	Unisys provides our response as follows.

Unisys Response:

Yes. Unisys provides Managed Security Services based on the approach outlined in our response to Q39, including the following clients:

- New York State
- Commonwealth of Pennsylvania
- City of Santa Clara
- City of Minneapolis
- California State University.

Q41.	Security	Have you supported Managed Security services in distributed environments - both physical and virtual including on premise and off premise implementations?	Unisys provides our response as follows.

Unisys Response:

Yes. We have supported MSS in distributed environments— both physical and virtual—including on-premise and off-premise implementations.

Our services can be delivered directly on the customer premise and throughout its distributed enterprise, in a distributed hybrid model between the customer premise and our security operations centers, or in the cloud.

Examples of on-premise implementations include the following clients:

- McDonalds
- City of Chicago
- U.S. Department of Agriculture.

Examples of off-premise implementations include the following clients:

- California State University
- City of Santa Clara
- Danone.

Physical security examples include the following clients:

- U.S. Customs & Border Protection
- U.S. Department of Defense
- U.S. Department of Homeland Security.

Q42.	Security	Do you offer solutions supporting geographically diverse locations (e.g., remote location with satellite)?	Unisys provides our response as follows.

Unisys Response:

Yes. Unisys MSS offerings will be connected to the Commonwealth's domain, typically through one or more IPsec VPN- or MPLS-based technologies.

Additionally, Unisys developed technology that can encrypt and cloak IP communications between end points on the same network and across diverse locations.

Unisys MSS offerings include the following elements:

- Managed Security Information and Event Management (SIEM)
- Security Device Management (SDM)
- Governance, Risk, and Compliance (GRC)
- Managed Identity and Access Management (IAM)
- Micro-segmentation (network-based segmentation based on user identity, not the traditional VLAN or firewall method of segmentation)
- Encryption for data in motion
- Highly automated PKI environment (Enterprise Key Management)
- Cloaking of IP communications to reduce the digital attack surface.

Q43.	Security	How have you implemented solutions similar to those in the Commonwealth making use of a centralized federated environment?	Unisys provides our response as follows.

Unisys Response:

The solutions that we list for the clients in our response to questions 41 include Managed SIEM, SDM, GRC, IAM, and Stealth technology.

Our approach includes the following elements:

- Consistent global ITIL processes: Our solution will use ITIL v3 for best practices, processes, and procedures.
- Service Quality through SLAs and SLRs: Our solution will verify that critical security life cycle, service management functions, and processes are defined with delineated roles and responsibilities, touch points, and measurements between the Commonwealth and Unisys.
- ISO 27001–certified Security Operations Centers: Unisys MSS provides security services from eight ISO 27001–certified Security Operations Centers (SOCs) around the globe that leverage ISO 9001, ITIL, and ISO 20000 international standards and best practices. To maintain our ISO certifications, we conduct annual internal security assessments and facilitate external independent verification and validation (IV&V) audits.

Exhibit A.2-1 illustrates our commitment, expertise, and country SOC locations that provide MSS around the world.

Q44.	Security	What do you consider to the be the key challenges and tradeoffs for	Unisys provides our response as follows.

		the implementation of Managed Security Services in an environment similar to the Commonwealth?	

Unisys Response:

If the MSSP Model is not adopted, the Commonwealth will have the following challenges:

- Diversity of IT security solutions, beliefs, and best practices across agencies
- Political boundaries and silos
- Inability to attract and retain top IT security talent
- Lack of 24x7 proactive threat intelligence and response
- Uneven governance, risk, and compliance
- Increased total cost of ownership for the Commonwealth (consider capex and opex)
- Inability to focus on core business and deliver products and efficient services to constituents.

If the MSSP Model is not adopted, the Commonwealth will have to consider the following tradeoffs:

- A decentralized, nonstandard suite of technology solutions and services
- Lack of qualified cybersecurity personnel.

If the MSSP Model is adopted, the Commonwealth will have the following challenges:

- Consolidating a wide variety of IT security solutions, beliefs, and best practices across agencies
- Current expenditure for hardware and software solutions and their life cycle
- Employee well-being—potential transfer to MSSP
- Uniformity of governance, risk, and compliance.

If the MSSP Model is not adopted, the Commonwealth will have to consider the following tradeoffs:

- Constituent data will be under SLA with MSSP
- TCO will be significantly reduced
- Jobs will be maintained—potential transfer to MSSP
- Uniform IT security across Commonwealth agencies
- 24x7 monitoring, response, and threat intelligence.

Q45.	Security	What do propose at a high level to be the key strategies and implementation elements of any typical security services solution migration?	Unisys provides our response as follows.

Unisys Response:

Unisys proposes the following key strategy:

- Review of the existing security framework
- Due diligence discovery process
  - Security assessment
  - Penetration testing
  - Identification of critical assets, users, etc.
- Design solutions
  - Consolidated design process
  - Reengineering and tooling
  - Automation options
- Implementation solutions
  - Development of technology integration requirements
  - Acceptance testing
- Sustainment of the Security Program
  - Design of management reports
- Development of Security Management dashboards

Unisys proposes a migration of our typical Security Services solutions with the following implementation elements:

- Security Device Management
- Security Information and Event Management (SIEM) Services
- Vulnerability Management Services and Support
- Vulnerability Scanning per Device
- Intrusion Detection System (IDS) and Intrusion Protection System (IPS) Services and Support
- Advanced Threat Analysis System Support Services
- Secure Web Gateway Services
- Threat Intelligence Services
- SOC Services
- Security Incidents (excludes false positives)
- Service Catalog Services.

Q46.	Security	Can you recommend additional Managed Security Services that are not currently included or considered in the scope of described services?	Unisys provides our response as follows.

Unisys Response:

Unisys recommends threat intelligence that is based on the most comprehensive, accurate, and actionable intelligence available, including intelligence gained from hacker forums, dark web, and social media. The scope of threats must include threat intelligence that is specifically pertinent to VITA in addition to intelligence pertaining to social-, infrastructure-, middleware-, and software-related threats.

To generate real-time, actionable intelligence, Unisys recommends that the service provider persistently monitor and analyze threat intelligence data sources through advanced statistical, linguistic, and crowdsourcing techniques. The actionable intelligence should focus on the integration of human, social network, and deep web-based intelligence sources fostering real-time decision making.

Examples of threat intelligence sources may include the following:

- Supercharging open source intelligence collection by monitoring social media, news, websites of interest, and the deep web
- Using sophisticated filtering based on date, language, sentiment, people, topics, keywords, etc.
- Geolocating social media postings to find people, validate access, and persistently stare at areas of interest
- Conducting link analysis—in minutes, not days—on individuals, groups, or corporations using integrated link analysis features
- Enhancing situational awareness through near-real time data collection and analysis
- Monitoring Internet relay chats and other deep web forums for mentions of nefarious activity such as terrorist planning, human trafficking, and cyberattacks
- Searching across more than 200 languages and translating on the fly—breaking dependency on linguists
- Developing pattern-of-life analysis for persons of interest
- Detecting social trends with sophisticated sentiment monitoring across multiple foreign languages.

Unisys also recommends that highly trained security analysts be certified and have the requisite clearances to provide briefings and interface with intelligence exchange communities (e.g., STIX and TAXII).

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?	Unisys provides our response as follows.

Unisys Response:

To overcome the key challenges, Unisys recommends that VITA ensure that the security services delivered by the provider comply with information security policies, standards, and regulatory requirements.

In accordance with our experience with similar public sector clients, Unisys recommends the following types of regulations, policies, procedures, and guidelines for consideration:

- Defense Information System (DIS)-200 information security and privacy standards, IRS Publication 1075, Criminal Justice Information Services (CJIS), Health Information Portability and Accountability Act of 1996/Health Information Technology for Economic and Clinical Health Act of 2009 (HIPAA/HITECH), Payment Card Industry Data Security Standard (PCI DSS), Family Educational Rights and Privacy Act (FERPA), and Minimum Acceptable Risk Standards for Exchanges (MARS-E) standards
- Assisting with the development of security standards, policies, and procedures that include industry best practices
- Providing a security plan based on Commonwealth-specified security requirements, architecture, standards, procedures, policies, local requirements, and risks
- Providing security incident severity-level classification, descriptions, and approach for managing and communicating incidents based on severity level
- Providing security reporting and communicating security breaches to the Commonwealth
- Recommending security changes based on industry best practices
- Providing security design and engineering to meet the Commonwealth's strategies and requirements as stated in the Master Agreement
- Participating actively in industry standard security forums and end-user groups to remain current with security trends, threats, common exploits, and security policies and procedures.

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?	Unisys provides our response as follows.

Unisys Response:

Unisys' best practice for delivery of MSS is that they be delivered remotely from one or more of our SOCs for the following reasons:

- Governance, risk, and compliance
- Evolving technology life cycle
- Centralized Managed Security Services
- Current technical security skills
- Ability to attract, train, and retain qualified resources.

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?	Unisys provides our response as follows.

Unisys Response:

In accordance with our current understanding of requested services, Unisys does not foresee the need for subcontractors. However, we reserve the right to change our opinion on subcontractors based on future changes to scope in the released RFP.

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 scope demarcation between potential RFPs.	Unisys provides our response as follows.

Unisys Response:

Because of the Commonwealth's vast physical and cybersecurity requirements, Unisys recommends that VITA separate the security RFP from the other towers.

The reason for this recommendation is so that the Commonwealth is enabled with the security delivery services required to meet the demands of a complex security environment. Each agency will require consistent, repeatable, predictive, and cost-effective services; the best way to meet that requirement is by delivering the services independently of the other towers.

D.	**Financial/Managed Security**		
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.	Unisys provides our response as follows.

		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, 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.	

Unisys Response:

Unisys is familiar and amenable to the proposed pricing structure. However, from an administrative perspective, we recommend a discussion focused on consolidating several of the data points (RUs). Additionally, we recommend modifying the pricing sheets to separate assets and capital from services. This would allow the Commonwealth to effectively manage the use of assets and services as required.

Unisys recommends that VITA describe the methodology for calculating the fees in Exhibits 4.1 and 4.2. The base charges, ARC, RRC, other unit rates, one-time charges, and other charge provisions set forth in these exhibits are intended to compensate the supplier for the resources used to provide the services. Additionally, these exhibits should describe the measures of resource use and the tracking of this use.

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?	Unisys provides our response as follows.

Unisys Response:

For items that are broken out into an RU structure, consistent with the Commonwealth's ARC/RRC tables, Unisys recommends truing up monthly or quarterly, which will ensure that the Commonwealth will be billed only for actual use.

Although Unisys is receptive to increased transparency, we want to avoid the potential administrative costs of reporting and billing on sub-RU elements.

Resource baselines identify the level of RUs that are included in the base charge for each RU for each month following the commencement date. Unisys recommends that the resource baselines should specify the quantity of RUs that are to be provided by the supplier each month for the base charges.

Examples include the following.

Security Information and Event Management (SIEM) Services. The Security Information and Event Management (SIEM) Services Resource Unit is defined as follows.

SIEM System Support Services

"SIEM System Support Services" shall be equal to:

- Ongoing management, support, and maintenance of the SIEM System, including Service Management responsibilities
- Ongoing performance and capacity monitoring and associated tuning for the SIEM System
- Ongoing operational alarm monitoring and resolution, including log sources that exceed agreed-upon log delay thresholds
- Installation of SIEM System patches, updates, and security content (e.g., rules, signatures) released by the SIEM System OEM
- Ongoing review and tuning of SIEM System event handling, rules, signatures and correlation (e.g., false positive tuning).

Events Per Second

"Events Per Second" shall be equal to the average number of raw events and logs (e.g., firewall syslog message) collected by the SIEM System per second.

This will be calculated by dividing the total number of events collected by the SIEM System for a given month by the number of seconds in that month.

Vulnerability Management Services

The Vulnerability Management Services Resource Unit is defined as follows.

Vulnerability Management Support Services

"Vulnerability Management Support Services" shall be equal to:

- Ongoing management, support, and maintenance of the Vulnerability Management System, including Service Management responsibilities
- Ongoing performance and capacity monitoring and associated tuning for the Vulnerability Management System
- Installation of Vulnerability Management System patches, updates and security content (e.g., vulnerability signatures) released by the Vulnerability Management System OEM
- Maintenance and updates for scanning configuration (discovery, vulnerability and configuration scanning), including targeted assets and IP ranges, configuration verification templates (e.g., configuration baselines) and scanning methods (e.g., authenticated versus unauthenticated)
- Performance of discovery scanning to identify unidentified hosts in Customer's Environment.

Vulnerability Scanning Per Device

"Vulnerability Scanning Per Device" shall be equal to the number of individual devices (i.e., hosts) successfully scanned for vulnerability and configuration compliance scanning during a given month. This includes initiating the remediation process for identified vulnerability and configuration issues through creation of Service Requests using Customer's Service Management Tool.

Intrusion Detection System (IDS) and Intrusion Protection System (IPS) Services. The IDS/IPS Services Resource Unit is defined as follows.

Network IDS/IPS System Support Services

"Network IDS/IPS System Support Services" shall be equal to:

- Ongoing management, support and maintenance of the Network IDS/IPS System, including Service Management responsibilities
- Ongoing performance and capacity monitoring and associated tuning for the Network IDS/IPS System
- Installation of Network IDS/IPS System patches, updates and security content (e.g., intrusion signatures) released by the Network IDS/IPS System OEM
- Ongoing review and tuning of Network IDS/IPS System policies and associated intrusion signatures / rules (e.g., false positive tuning)

Network IDS/IPS Sensors

"Network IDS/IPS Sensors" shall be equal to the number of Network IDS/IPS sensors (i.e., appliances) installed and active in Customer's Environment as of the last day of the given month.

Advanced Threat Analysis System Support Services

"Advanced Threat Analysis System Support Services" shall be equal to:

- Ongoing management, support and maintenance of the Advanced Threat Analysis System, including Service Management responsibilities
- Ongoing performance and capacity monitoring and associated tuning for the Advanced Threat Analysis System
- Installation of Advanced Threat Analysis System patches, updates and security content (e.g., intrusion signatures) released by the Advanced Threat Analysis System OEM
- Ongoing review and tuning of Advanced Threat Analysis System policies and associated intrusion signatures and rules (e.g., false positive tuning).

Advanced Threat Analysis System Sensors

"Advanced Threat Analysis System Sensors" shall be equal to the number of Advanced Threat Analysis System sensors (i.e., appliances) installed and active in Customer's Environment as of the last day of the given month.

Secure Web Gateway Services. The Secure Web Gateway Services Resource Unit is defined as follows.

Secure Web Gateway Services

Secure Web Gateway Services include up to 10,000 Authorized Users. "Secure Web Gateway Services" shall be equal to:

- Ongoing management, support and maintenance of the Secure Web Gateway System (includes associated log retention and reporting system), including Service Management responsibilities
- Ongoing performance and capacity monitoring and associated tuning for the Secure Web Gateway System
- Installation of Secure Web Gateway System patches, updates and security content (e.g., URL filtering categorization, anti-malware engine signatures) released by the Secure Web Gateway System OEM
- Ongoing review and tuning of Secure Web Gateway System policies.

Threat Intelligence Services. The Threat Intelligence Services Resource Unit is defined as follows.

Threat Intelligence Support Services

"Threat Intelligence Support Services" shall be equal to:

- Ongoing analysis and reporting of current threats
- Ongoing configuration of Threat Intelligence Service to incorporate Customer's Business and IT environment, including vulnerability and configuration management data
- Ongoing recommendation and implementation of rules, policies, signatures and tuning in response to identified threats
- Providing Customer with the ability to access and query threat intelligence information.

SOC Services. The SOC Services Resource Unit is defined as follows.

Security Incidents (Excludes False Positives)

"Security Incidents (Excludes False Positives)" shall be equal to the number of Security Incidents Resolved in the given month by the Supplier in Customer's Security Incident Management System. Security Incidents identified as false positives will be excluded.

Service Catalog Services. The following "Service Catalog Services" shall be provided according to the descriptions in Exhibits 4.1 and 4.2:

- SIEM Log Source Installations Requests
- SIEM Log Source Decommissions Requests
- Secure Web Gateway System Custom Filtering Requests
- Custom Signatures Requests
- Custom Threat Intelligence Research/Report Requests
- Ad Hoc Vulnerability Scan and Scan Results Report Requests.

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.	Unisys provides our response as follows.

Unisys Response:

Unisys has considerable experience with managing, acquiring, and procuring assets for our clients. Because the Commonwealth does not wish to own its assets and some assets owned by the incumbent may have useful life, we recommend a flexible arrangement in which the Commonwealth would partner with the vendor of the assets or a third-party financial partner to limit capital exposure to the Commonwealth and minimize ongoing expenses. The cost recovery for these assets would be built into the base charges or milestones. Unisys looks forward to a detailed discussion on asset ownership.

FEEDBACK REGARDING RFI DOCUMENTS

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

<table>
<tr><th>Ref#</th><th>Document/Section</th><th>Supplier Commentary</th></tr>
<tr><td>C1.</td><td>Document: VITA-RFI 2017-14 – 04.2-a; Section:2.1.2</td><td>As the Commonwealth considers server RUs and pricing, Unisys recommends considering the use of standardized server specifications that can be assigned to a size definition, such as small, medium, and large, especially when planning technology refreshes and migrations to the cloud or other data center environments. By using standardized specifications, the Commonwealth will gain increased cost management due to consistent volume for hardware vendors and reusability of the assets. Additionally, as workloads are migrated to the cloud, the configurations will be able to be transferred between the virtualization, private cloud, and public/Commonwealth cloud environments consistently and provide a basis for evaluated costs because the configurations will be similar in each environment.</td></tr>
<tr><td>C2.</td><td>Document: VITA-RFI 2017-14 – 04.2-a; Section: 2.2.1</td><td>Unisys recommends that the Commonwealth provide information on each of the storage tiers. This information can help to support the Commonwealth’s goal for maintaining performance and improve transparency of the structure for the solutions.

The following table is an example of the information the Unisys recommends to include for Storage services. Based on the differences that occur between the centralized and noncentralized data centers, these performance criteria may vary by environment.
<table>
<tr><th>Storage Tier</th><th>Expected IOPS/TB in the Storage Tier</th><th>Average IOPS/MBPS Per Server</th><th>Latency/Delay (ms)</th></tr>
<tr><td>Tier 0 SAN (Flash)</td><td>3,000</td><td>50,000 IOPS</td><td>< 1</td></tr>
<tr><td>Tier 1 SAN</td><td>1,000</td><td>8,000 IOPS</td><td>4</td></tr>
<tr><td>Tier 2 SAN</td><td>400</td><td>600 IOPS</td><td>8</td></tr>
<tr><td>Tier 3 SAN (Archive)</td><td><100</td><td>500 IOPS</td><td>10</td></tr>
<tr><td>Tier 1 NAS</td><td>400</td><td>80 MBPS</td><td>4</td></tr>
<tr><td>Tier 3 NAS</td><td>150</td><td>40 MBPS</td><td>8</td></tr>
<tr><td>Tier 3 NAS</td><td><50</td><td>30 MBPS</td><td>10</td></tr>
</table></td></tr>
</table>

<table>
<tr><td>C3.</td><td>Document: VITA-RFI 2017-14 – 04.2-a; Section: 2.2.2</td><td>In addition to the current definition of backups being related on a one to one basis to the “active GB Protected,” Unisys recommends providing definitions for retention requirements. Several regulations and business operations require extended retention of data beyond an average data protection life cycle based on 30- or 60-day retention. As a result, Unisys recommends considering additional RUs to establish common predefined retention policies aligned with the regulations for transparency to the vendor community and the Commonwealth agencies.</td></tr>
<tr><td>C4.</td><td>Document: VITA-RFI 2017-14 – 04.2-a; Section: 2.3</td><td>As stated in Q19, the Commonwealth uses a traditional monolithic single data DR model. In order to transform to support DR for facility disasters and business conditions, Unisys recommends providing a multitier model that includes requested RPOs and RTOs. By providing the expected DR tiers to the vendor community, the Commonwealth will be able to evaluate the solutions consistently and have a clear view of the services being offered.

The following table is an example of the information that Unisys recommends to include for DR services.
<table>
<tr><th>DR Tier</th><th>RPO (Hrs)</th><th>RTO (Hrs)</th><th>Strategy</th></tr>
<tr><td>0</td><td>Near 0</td><td>4</td><td>Online storage replication with distance limitation from production to DR site

Server: Hot</td></tr>
<tr><td>1</td><td>1</td><td>4-12</td><td>Online storage replication

Server: Hot/Warm</td></tr>
<tr><td>2</td><td>1</td><td>24</td><td>Replication and recovery

Server: Warm/Cold</td></tr>
<tr><td>3</td><td>24</td><td>36</td><td>Disk-based backup recovery and replication

Server: Warm/Cold</td></tr>
<tr><td>4</td><td>24</td><td>72</td><td>Tape-based backup data recovery

Server: Cold</td></tr>
</table></td></tr>
</table>

The following table provides definitions for the server recovery strategies.

Server Recovery	OS License Requirement	Compute and Storage	Requirements
Cold	None	Reserved	Assignment, allocation, and configuration of server, network, and other infrastructure during DR Test and Events
Warm	Yes	Yes	Configuration updates for application, server, network, and other infrastructure during DR Test and Events
Hot	Yes	Yes	Server, network, and other infrastructure setup to support day-to-day operations, DR Test, and Events

C5. Managed Security Services Section

Unisys implemented MSS best practices internally and across our solution offerings. We provide MSS to multiple clients globally across the Commercial, Public Sector, and Federal/National Government market segments. We strongly recommend that VITA issue a separate RFP for MSS. In that context, we think that it would be helpful to share a best practices example of MSS RFP content outline for VITA's use. We are available to discuss this outline in more detail at VITA's request. We are also willing to provide additional MSS analysis support to the extent that it would not interfere with our ability to respond to the forthcoming RFP.

Exhibit/Attachment Number	Title	Bidder Response Required? Yes/No
N/A	Executive Summary	Yes
Appendix A to the RFP Introduction and Instructions	Acknowledgement Form	Yes
Appendix B to the RFP Introduction and Instructions	Tools Recommendation and Pricing	Yes
Appendix C to the RFP Introduction and Instructions	ALCS Technical Environment and Volumes	No
Appendix D to the RFP Introduction and Instructions	Firewall and NAC Service Capabilities	Yes

N/A	Master Agreement	Yes
Exhibit 1	Definitions	Yes
Exhibit 2.0	Services	No
Exhibit 2.1	Statement of Services – Managed Security Services	Yes
Exhibit 2.2	Statement of Services – Cross Functional Services	Yes
Exhibit 3	Service Levels	Yes
Attachment 3-A	Service Level Matrix	Yes
Attachment 3-B	Service Level Examples	No
Attachment 3-C	Priority Levels	Yes
Attachment 3-D	Measurement Tools and Methodologies	Yes
Attachment 3-E	Maximum Permitted Failovers	Yes
Exhibit 4	Pricing and Financial	Yes
Attachment 4-A	Supplier Pricing and Baselines	Yes
Attachment 4-B	Financial Responsibility Matrix	Yes
Attachment 4-C	Market Currency Procedures	Yes
Exhibit 5	Personnel Projection Matrix, Supplier Locations and Supplier Space Requirements	Yes
Exhibit 6	Governance Model	Yes
Exhibit 7	Sites	No
Exhibit 8	Standards	No
Exhibit 9	Projects	No
Attachment 9-A	Active Projects	No
Attachment 9-B	Planned Projects	No
Exhibit 10	Equipment Assets	Yes
Exhibit 11	Software Assets	Yes
Exhibit 12	Third Party Contracts	No
Exhibit 13	Reports	Yes

Exhibit 14	Key Supplier Employees	Yes
Exhibit 15	Policies (including all Attachments)	Yes
Exhibit 16	Listed Subcontractors	Yes
Exhibit 17	Transition/Implementation Plan	Yes
Attachment 17-A	Transition Deliverables	Yes
Attachment 17-B	Technical Solution Document	Yes
Exhibit 18	Termination Assistance Services	Yes
Exhibit 19	Customer Group Competitors	No
Exhibit 20	Disaster Recovery / Business Continuity	Yes