



**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](mailto: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.....	3
A. IT Infrastructure Services Program (ITISP) Overview .....	3
B. RFI Purpose.....	3
2. Submission Logistics and Contact Information .....	5
3. Overview of RFI Documents .....	5
4. Respondent Contact Information.....	6
5. Questions.....	7
A. Server/Storage Services.....	7
B. Financial/Server Storage .....	16
C. Managed Security.....	18
D. Financial/Managed Security .....	32
6. Feedback Regarding RFI Documents .....	35

## 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 4<sup>th</sup> 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 (CSR)M) 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

---

<b>Issue Date:</b>	September 29, 2016
<b>Due Date / Time:</b>	October 21, 2016 at 3:00 pm EST
<b>Response Delivery Method:</b>	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.
<b>Single Point of Contact (SPOC):</b>	Greg Searce
<b>Telephone:</b>	(804) 416-6166
<b>E-mail Address:</b>	<a href="mailto:gregory.searce@vita.virginia.gov">gregory.searce@vita.virginia.gov</a>
<b>Mailing Address:</b>	11751 Meadowville Lane, Chester, VA 23836
<b>Pricing:</b>	No pricing information should be submitted
<b>Document Format:</b>	Return this document, having populated Section 4 (Respondent Contact Information), Section 5 (Questions) below, and Section 6 (Feedback Regarding RFI Documents)
<b>RFI Questions and Answers:</b>	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	Accenture PLC
Company Mailing Address	161 N Clark St, Chicago, IL 60601
Company Website Address	Accenture.com
Name of Contact Person	Damian A. Kelly
Contact Person E-mail Address	damian.a.kelly@accenture.com
Contact Person Telephone #	+1 919-899-3906

## 5. QUESTIONS

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

Ref#	Category	Question	Supplier Response
<b>A. Server/Storage Services</b>			
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?	Accenture is not responding to this section
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.	Accenture is not responding to this section
Q3.	Data Center	What do you recommend for the length of the contract for the Data Center Facility for this type of environment?	Accenture is not responding to this section
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?	Accenture is not responding to this section
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?	Accenture is not responding to this section
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?	Accenture is not responding to this section
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?	Accenture is not responding to this section
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?	Accenture is not responding to this section
Q9.	Server/Storage	Do you see a better way to bundle or spilt the services we are	Accenture is not responding to this section

Ref#	Category	Question	Supplier Response
		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?	
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?	Accenture is not responding to this section
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?	Accenture is not responding to this section
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.	Accenture is not responding to this section
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)?	Accenture is not responding to this section
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?	Accenture is not responding to this section
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?	A Key Management solution that can manage certificates and keys for the applications and services running in the cloud as well as on-premises is a critical aspect of enterprise security. Accenture has a robust and end to end key management capability that not only provides a centralized control over the encryption keys, but also takes care of the more onerous scalability and availability issues that inevitably surface when you implement key management at enterprise scale. Following are the details on the Accenture's key management service (service capabilities, estimation

Ref#	Category	Question	Supplier Response
			<p>factors. Deployment models etc.) that accounts for the factors that Commonwealth can consider as it requests for this service:</p> <p><b><u>Accenture’s Key Management Service:</u></b>                      Managed PKI service provides key management and digital certificates for clients. This service caters to application hosted premises and in the cloud environment.</p> <p><b><u>Service Description, Provides:</u></b></p> <ul style="list-style-type: none"> <li>• PKI Infrastructure including digital certificate and key management</li> <li>• Certificate enrollment and registration services</li> <li>• Configuration and trusted root signing</li> <li>• Configuration backup and restore management</li> <li>• User management and registration services</li> <li>• Customized reporting and dashboard</li> </ul> <p><b><u>Estimation Parameters:</u></b></p> <ul style="list-style-type: none"> <li>• Number of Applications</li> <li>• Number of PKI certificates to be managed</li> <li>• Certificate expiration cycle</li> </ul> <p><b><u>Deployment Model:</u></b></p> <ul style="list-style-type: none"> <li>• As a Service (MSO @ Accenture)</li> <li>• CPE (MSO @ Customer)</li> </ul> <p><b><u>Service Window</u></b></p> <ul style="list-style-type: none"> <li>• 24 x 7 or</li> <li>• 8 x 5</li> </ul> <p><b><u>Product Support:</u></b></p>

Ref#	Category	Question	Supplier Response
			<ul style="list-style-type: none"> <li>• Entrust</li> <li>• Client specific technology</li> </ul> <p><b>Platform Support:</b></p> <ul style="list-style-type: none"> <li>• On Premises Applications</li> <li>• Cloud Applications</li> </ul>
Q16.	MSI	<p>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?</p>	<p>Accenture recommends a multi-phased approach that includes defining the key requirements and blueprint for the IAM solution along with the analysis of current IAM services to develop the integration plan and migration strategy. Accenture could help the Commonwealth protect its investments in the IAM toolset and could use the existing services for various transformation initiatives.</p> <p>The Accenture team will start the transformation journey with a definition of IAM strategy to align with the business objectives of Commonwealth.</p> <p><b>Activities:</b></p> <ul style="list-style-type: none"> <li>• Understand and document the current IAM environment including inventory of the existing IAM toolset</li> <li>• Understand and document future business requirements from an identity and access management standpoint</li> <li>• Conduct a gap assessment of current state and the desired future state</li> <li>• Define a solution blueprint for the future state</li> <li>• Define the roadmap to transform from the current state to the future state</li> <li>• Recommend any additional tools required for the transformation</li> </ul>

Ref#	Category	Question	Supplier Response
			<ul style="list-style-type: none"> <li>• Define a governance structure to manage the transformation</li> <li>• Present the IAM strategy to Commonwealth and gain approval</li> </ul> <p>Our approach would be in stages, firstly to rationalize the differing identity providers moving towards a federative trust model, secondly a transformation activity to provide a single integrated identity and access service. These activities would include the following stages:</p> <ul style="list-style-type: none"> <li>- Assess current identity providers - Understand Current State, Assess Current Infrastructure and Conduct interviews &amp; Document Observations.</li> <li>- Define an approach towards integration. Steps could include: <ul style="list-style-type: none"> <li>o Federation of multiple providers to provide a unified trust model as a first step if necessary. This may be done to provide the basis on which user rationalization can occur. An initial step using identity federation allows users to consolidate the many local identities they have configured among multiple service providers. With one federated identity, the user can log in at one service provider's site and move to an affiliated service provider site without having to re-authenticate or re-establish identity. Identity Federation services can work with SAML to enable single sign-on sessions among business partners. The Identity Federation services normally consists of a web service</li> </ul> </li> </ul>

Ref#	Category	Question	Supplier Response
			<p>interface, a core Identity Federation component, and an Identity Federation Framework that complies with client specifications.</p> <ul style="list-style-type: none"> <li data-bbox="1415 337 1906 1252">○ Virtualization of identity sources with a single unified identity provider. This approach is often popular when identity sources need to remain in place for legacy reasons with complex directory customizations. This also could be considered as an intermediate step towards unification. A common approach for this step is to migrate applications in a prioritized manner to the virtualized directory service, migrating their identity management and access control to the new system, but leaving back end integrations to applications. Virtualization technologies allow for high availability, high speed presentation of secure directory services presenting a single unified LDAP to the identity service, while being integrated and connected to multiple existing directory services including LDAP, Active Directory, Databases or even flat files.</li> <li data-bbox="1415 1263 1906 1463">○ Rationalization of identity sources into single unified model. This involves bringing in all identity providers and their identity sources into a single provider model. As new systems are implemented, they</li> </ul>

Ref#	Category	Question	Supplier Response
			<p>would be integrated directly to the new unified model. A selection process would determine existing systems which need to be rationalized at the application side and older systems which may be left in the virtualized directory until they are decommissioned.</p> <ul style="list-style-type: none"> <li>- Define integration roadmap. This will take into account the approach, and which intermediate steps towards full rationalization are needed.</li> <li>- Implement integration approach over the duration of the roadmap. This includes all identity migration, rationalization and reconciliation activities associated.</li> </ul> <p>As one of the trusted service providers, Accenture is positioned to help the Commonwealth achieve these objectives, offering unique advantages that include:</p> <ul style="list-style-type: none"> <li>• Our Approach – Our experience with outsourcing our client’s critical processes enables us to bring field-tested service transition methodology and delivery approaches which minimize disruption and provide high-quality service as expected.</li> <li>• IAM Experience – We have performed these services for other public sector clients of similar size and complexity to the Commonwealth, and are able to leverage the Accenture practices and people that have made those projects successful for this engagement. Accenture has industry recognized strength as an IAM managed and security outsourcing services provider</li> </ul>

Ref#	Category	Question	Supplier Response
			<p>complimented with strong transition, service integration services, and a track record for consistently delivering quality.</p> <ul style="list-style-type: none"> <li>• Continuous Improvement through Industry Leading Innovation - We would leverage onsite IAM advisors early in the “transition” phase of our engagement to outline ideas for continuous improvement and automation to accelerate efficiencies in the “run” phase.</li> <li>• Outcomes based - Rather than just consolidating IAM Operations service providers and headcount, we propose to implement a model based on results and service level agreements</li> </ul>
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?	Accenture is not responding to this section
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)?	Accenture is not responding to this section
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?	Accenture is not responding to this section
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?	Accenture is not responding to this section
Q21.	Migration	Suppliers will be required to provide an implantation plan to specify	Accenture is not responding to this section

Ref#	Category	Question	Supplier Response
		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?	
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?	Accenture is not responding to this section
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?	Accenture is not responding to this section
Q24.	Enhanced Services	What would you propose as a good business case for virtualizing the desktop (offering VDI)?	Accenture is not responding to this section
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.	Accenture is not responding to this section
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?	Accenture is not responding to this section
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?	Accenture is not responding to this section
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?	Accenture is not responding to this section
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?	Accenture is not responding to this section

Ref#	Category	Question	Supplier 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?	Accenture is not responding to this section
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?	Accenture is not responding to this section
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?	Accenture is not responding to this section
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?	Accenture is not responding to this section
Q34.	Cloud Services	When the Commonwealth buys cloud services offerings how do you propose to identify where the data and services are located?	Accenture is not responding to this section
<b>B. Financial/Server Storage</b>			
Q35.	Pricing Structure	<p>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.</p> <p>The Commonwealth will contemplate any proposed pricing structure along five dimensions:</p> <ol style="list-style-type: none"> <li><b>Predictable:</b> 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.</li> <li><b>Manageable:</b> 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.</li> </ol>	Accenture is not responding to this section

Ref#	Category	Question	Supplier Response
		<p>3. <b>Fair:</b> 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.</p> <p>4. <b>Incentives:</b> 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.</p> <p>5. <b>Flexible:</b> 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.</p>	
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?	Accenture is not responding to this section
Q37.	Asset Ownership	The Commonwealth consumes certain services today which are underpinned by a set of assets (servers, firewalls, etc.). The	Accenture is not responding to this section

Ref#	Category	Question	Supplier Response
		<p>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.</p>	
<b>C. Managed Security</b>			
Q38.	Security	<p>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?</p>	<p>Accenture understands that organizations face a number of key challenges around security and risk functions supporting the achievement of business objectives. Accenture Managed Security Services has the capability to provide end-to-end managed security services and we do not foresee any significant challenges in providing security services around this bundled model. We have always advocated a defense-in-depth approach to security and the results of our vulnerability assessments have enabled us to design remediation roadmaps and implementation plans to help our clients improve those areas of security that represented the greatest risks to the organization. Bringing various functions of security into an integrated model would provide single view to risk posture.</p> <p>Security is a key component within Accenture Operations and we have formed a market leading Security Practice offering the services to help organizations address all of their security needs.</p> <p>Accenture Managed Security Services (MSS) provides organizations with the ability to rapidly scale security and compliance operations. It supports the digital enterprise by providing innovative technologies, top security talent, and an operating model that is</p>

Ref#	Category	Question	Supplier Response
			<p>designed to provide measurable business outcomes.</p> <p>MSS provides integrated end-to-end security services for large enterprise clients at the global and regional levels. Accenture's approach is based on consulting led transformation for optimized and high performing security operations aligned to our client's respective industries. MSS transformation framework and industrialized offerings enable consistent delivery and improved client experience for defending digital business.</p> <p>Our MSS Go-To-Market strategy is aligned with Accenture's overall strategy to support clients in each of the industry verticals. Our Clients are typically large enterprise customers who look at security as a core business enabler.</p> <p>MSS operations is delivered through our Cyber Fusion Centers globally. Our Centers combine innovation and incubation (Labs), proof of concept (Liquid Studios) and the industrialization, scale and ongoing delivery of security services, as-a-Service. Our service delivery also brings together or fuses our end-to-end security capabilities spanning our entire business, giving clients direct, one stop access to our strategic, transformational and operational security services. Accenture's Managed Cyber Defense Platform provides enterprise visibility, threat intelligence, and guided remediation of threats and vulnerabilities.</p>
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?	Accenture has performed a number of roadmap projects for recommending to our clients how to scale up their existing security landscape. Our typical deliverables on such a project include a solution blueprint, depiction of the current and the future

Ref#	Category	Question	Supplier Response
			<p>state, identification of work packages to address the gaps and an effort estimation for each of the work packages.</p> <p>Accenture takes a structured approach to measure and improve the security environment of organizations of the size and complexity similar to that of Commonwealth. Our framework is based on the ITIL framework for Continuous Improvements and anchored around an Industrialization program called "Delivery Industrialization and Innovation Program." This framework provides access to Accenture experience and field-tested practices across clients and provides a standard way of implementing service improvement roadmaps across delivery teams. Our Service Performance metrics are continuously reviewed and revised based on our capability upgrades and our performance benchmarks.</p>
Q40.	Security	<p>Can you provide examples of comparable environments where you offer security services similar to those required by the Commonwealth?</p>	<p>Accenture’s experience in delivering Enterprise Security-as-a-Service and managed security service solutions draws on the experience Accenture has gained from hundreds of clients globally.</p> <p>Accenture brings a team with the breadth of relevant experience comparable to what the Commonwealth is looking for. Accenture client references reflect both the diversity of the clients served and the security experience required to deliver this project on time and on budget. The following table demonstrates Accenture’s ability to perform the scope of work described in this RFI.</p> <div data-bbox="1264 1404 1913 1448" style="background-color: #4F81BD; color: white; text-align: right; padding: 5px;"> <b>Requirement Scope</b> </div>

Ref#	Category	Question	Supplier Response						
			Projects	Threat Identification or Prevention or Detection Penetration/Vulnerability	Set-up Penetration/Vulnerability	Testing Infrastructure Security Audit Services	Active Threat, Vulnerability, Penetration Remediation	Remediation Set-up	Remediation Action
			State of Ohio – Security Assessments, System Security Plan, and Security Services	✓			✓	✓	✓
			State of California, “Partner Agencies”: Department of Finance, State Controller’s Office, State Treasury Office, and Department of General Services (CA FI\$CAL)	✓	✓	✓	✓	✓	✓
			State of Florida (Florida Retirement System) – IT Security Risk and Vulnerability Assessment		✓	✓	✓	✓	✓
			State of Idaho—YHI Security Management		✓	✓	✓	✓	✓
			State of Iowa—Department of Human Services (DHS)		✓	✓	✓	✓	✓

Ref#	Category	Question	Supplier Response
			<p data-bbox="1276 203 1493 256">U.S. Department of Veterans Affairs</p>  <p data-bbox="1264 321 1892 678">Accenture has included relevant experience / case studies for the Commonwealth that showcase our experience in providing Managed Security Services. Security components of these case studies illustrate services that include security architecture, deployment, and management of security devices and systems, infrastructure security, Identity and Access Management, Threat and Vulnerability management, Incident response and overall security compliance.</p> <div data-bbox="1339 711 1606 776">   </div> <p data-bbox="1264 781 1654 829">Managed Security Services Comparable Accenture Client Credentials.docx</p>
Q41.	Security	<p data-bbox="407 987 1234 1089">Have you supported Managed Security services in distributed environments - both physical and virtual including on premise and off premise implementations?</p>	<p data-bbox="1264 847 1906 1230">Yes; Accenture has experience and expertise in providing Managed Security services in distributed environments - both physical and virtual including on premise and off premise implementations. We are working with some of the State Government agencies on a hybrid model with some of the security resources working on premise with the client and rest of the resources working from remote Accenture Delivery locations. Based on the requirements, Accenture would develop a model to suit the needs of the Commonwealth.</p>
Q42.	Security	<p data-bbox="407 1312 1192 1377">Do you offer solutions supporting geographically diverse locations (e.g., remote location with satellite)?</p>	<p data-bbox="1264 1279 1906 1440">Accenture has the capability and global presence to support geographically diverse locations. Accenture’s Managed Security Services are delivered from 14 locations across the globe and they operate 24 hours a day and 365 days a year. The delivery locations</p>

Ref#	Category	Question	Supplier Response
			<p>have enhanced physical and logical access controls, deep-skilled resources, and are equipped with next generation security management frameworks. Our Security Operations Centers coordinates and provides technical expertise and leadership oversight utilizing agreed-upon processes and communication channels to address security threats and deliver solutions to geographically diverse locations.</p>
Q43.	Security	<p>How have you implemented solutions similar to those in the Commonwealth making use of a centralized federated environment?</p>	<p>Accenture has extensive experience implementing and managing solutions similar to those in the Commonwealth making use of a centralized federated environment. Please review the response to question 40 above for complete details</p>
Q44.	Security	<p>What do you consider to be the key challenges and tradeoffs for the implementation of Managed Security Services in an environment similar to the Commonwealth?</p>	<p>Accenture has years of industry experience in providing Managed Security Services to global clients in an environment similar to that of the Commonwealth that has helped us to identify key implementation challenges such as:</p> <ul style="list-style-type: none"> <li>•Insufficient availability of knowledgeable resources from Client Incident Detection and Response or Accenture’s MSO teams to support the Build and Initial Operations efforts.</li> <li>•Insufficient availability of Client business, security and technical resources for review and sign-off of project deliverables and stage/gate approval.</li> <li>•Acceptance and resistance risk (insufficient cooperation from MSI and other stakeholders).</li> <li>•Unforeseen delays in the approvals of changes for the implementation.</li> <li>•Acceptance of Client Business IT for integrating applications with SIEM solution.</li> <li>•Unnecessary rules activated on the SIEM, resulting in high number of alert noise.</li> <li>•Confirming audit compliance</li> <li>•Reducing enterprise risk</li> </ul>

Ref#	Category	Question	Supplier Response
			<ul style="list-style-type: none"> <li>• Commitment to protecting the confidentiality, integrity, and availability of its data</li> <li>• Increasing volumes of stored sensitive data.</li> <li>• Lead time for mobilizing resources onsite/offsite</li> <li>• Transfer phase lengthy and potentially disruptive to operations</li> <li>• Tracking and measuring knowledge transfer progress is complex and difficult</li> <li>• Visas and extensive travel required for many team members</li> <li>• Knowledge transitioned on “one-off” basis, repetition frequently required.</li> </ul>
Q45.	Security	<p>What do propose at a high level to be the key strategies and implementation elements of any typical security services solution migration?</p>	<p>At a high level, the key strategies and implementation elements of any typical security services solution migration should include:</p> <p>Security Services focus on three key areas:</p> <ol style="list-style-type: none"> <li>1. Risk Management services provide the comprehensive visibility of the enterprise through vulnerability management, security event monitoring, security log review, incident response, and security compliance monitoring.</li> <li>2. Identity and Access Management services include self-service password management, directory management, identity lifecycle management, certificate management, and strong authentication.</li> <li>3. Infrastructure Security services focus on the management and administration of core infrastructure security devices, such as intrusion detection and prevention systems and firewalls.</li> </ol> <p>Accenture’s methodology includes a Service Transition readiness assessment that addresses the</p>

Ref#	Category	Question	Supplier Response
			<p>following areas:</p> <ul style="list-style-type: none"> <li>• Sponsorship - Every Security service must have at least one owner who is respectively are accountable for the business value and underpinning technology</li> <li>• Stability -The product or service must be subject to a low failure rate and a low probability of functional or technical change in the period immediately following go-live.</li> <li>• Operability -Service Delivery must be able to operate the system under normal day-to-day conditions with reasonable operator effort using an approved staffing and skills profile.</li> <li>• Maintainability - Documentation and support tools must be adequate Service delivery must be able to make emergency and permanent fixes the agreed staffing profile.</li> <li>• Performance -Target service levels must have been formally agreed with the client, and the product or service must be able to meet these reliably with a reasonable amount of support resource. This includes monitoring and adequate, tested contingency procedures</li> <li>• Recoverability -Service Delivery must be able to recover the service from hardware or software faults, with reasonable effort using agreed staffing profile and within an agreed time frame.</li> <li>• Information Security - The requirements for security, integrity, and controls must be met by the design and implementation.</li> <li>• Controls -The product or service must be subject to control using the support</li> </ul>

Ref#	Category	Question	Supplier Response
			<p>processes established (i.e., Release-, Change-, Incident-, and Availability Management).</p> <p>Service Readiness Checklist:</p> <ul style="list-style-type: none"> <li>• Training Materials</li> <li>• Service Documentation</li> <li>• Operations Acceptance Plan</li> <li>• Operations Acceptance Criteria</li> <li>• Operations Acceptance Report</li> <li>• Known Error Record</li> <li>• Exception Process</li> <li>• Service Readiness Plan</li> <li>• Service Rehearsal Plan</li> <li>• Service Rehearsal Materials</li> <li>• Service Rehearsal Report</li> <li>• Service Readiness Report</li> </ul>
Q46.	Security	<p>Can you recommend additional Managed Security Services that are not currently included or considered in the scope of described services?</p>	<p>Based on the high level analysis of the requirements, Accenture proposes that the Commonwealth move from operational security to a more advanced Security Analytics and Threat Hunting approach. We need to understand additional details of the environment to propose a detailed solution.</p> <p>Here’s what Accenture proposes based on our Cyber Defense Platform which is a solution that uses the latest industry leading software companies and combines all of their best attributes to build a comprehensive cyber solution tied together with Accenture intelligence.</p> <p><b><u>Security Analytics, incident management, and evolution with Splunk:</u></b></p> <ul style="list-style-type: none"> <li>• At its core, any great Cyber offering needs a back end to pull all of the data feeds together to create the ability to find and respond to potential threats. Splunk provides a</li> </ul>

Ref#	Category	Question	Supplier Response
			<p>foundation that ties into nearly all infrastructure items.</p> <ul style="list-style-type: none"> <li>• Perimeter defense, traffic evaluation, threat intelligence with Palo Alto:</li> <li>• The most basic tenant of Cyber Security is to mitigate the ability for threats to enter a network. In this regard Palo Alto with the Next Generation Firewall, Autofocus threat intelligence, and wildfire malware analysis fits perfectly and ties back into Splunk.</li> <li>• Endpoint Protection, Asset management, and incident response with Tanium:</li> <li>• The final piece to the puzzle is the individual components of the internal endpoints. It is imperative that these be managed, protected, and evaluated at scale. Tanium is the leader in this area due to their 15 second ability. This creates a scalable environment that allows for efficient response.</li> </ul> <p><b>FusionX</b> – Advanced Adversary Simulation  Our clients engage us to evaluate and improve their ability to prevent, detect, and respond to attacks against their most critical information assets  Our Unique Offering Includes:  Deep Offensive Expertise</p> <ul style="list-style-type: none"> <li>• Senior team with 10+ years in offensive operations</li> <li>• White-glove approach &amp; ability to operate in business-critical production environments with no operational impact</li> <li>• Accurate emulation of the adversary’s tactics, techniques, and procedures (TTP’s) tailored to each assessment</li> <li>• Scenario-based assessments</li> </ul>

Ref#	Category	Question	Supplier Response
			<ul style="list-style-type: none"> <li>• Full-Scope Attack Simulations               <ul style="list-style-type: none"> <li>• External &amp; Internal Network Penetration</li> <li>• Social Engineering &amp; Advanced Spear Phishing</li> <li>• Physical Penetration &amp; Device Planting</li> <li>• Long-Term Persistent Threat Simulation</li> <li>• ... all blended together into a coordinated attack simulation</li> </ul> </li> <li>• High-Stealth Approach               <ul style="list-style-type: none"> <li>• Zero-Notice, Zero-Knowledge assessments provide an accurate measure of your ability to detect &amp; respond to advanced attacks</li> <li>• FusionX provides a realistic sparring partner for the security operations team</li> <li>• Out-brief with the security operations team fosters continual detection &amp; response improvement</li> </ul> </li> <li>• Operations Backed by Advanced R&amp;D               <ul style="list-style-type: none"> <li>• Highly-skilled internal research team develops custom Oday exploits, command &amp; control payloads, and persistence frameworks tailored to our target environments</li> <li>• These technologies accurately simulate capabilities employed by advanced adversaries and allow FusionX to bypass many preventative and detective security control</li> </ul> </li> </ul> <p><b><u>Threat Hunting as-a-service</u></b>            Accenture and Endgame Inc., a leading provider of security solutions designed to proactively evict adversaries, have created a threat hunting as-a-Service offering for clients. Powered by Endgame and operated by Accenture senior cybersecurity hunters, the powerful service stealthily helps to identify and</p>

Ref#	Category	Question	Supplier Response
			<p>surgically remove known and never before seen adversaries that have evaded traditional security methods.</p> <p>Core to the offering are Accenture's seasoned global cybersecurity hunters, whose deep experience enables them to identify and terminate the efforts of latent attackers targeting organizations' intellectual property, business systems or other key assets. Clients can benefit from continuous business operation, free from disruption faced by users of traditional security approaches, who are typically under siege for months as they try to identify and remediate sophisticated adversaries.</p>
Q47.	Security	<p>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?</p>	<p>Accenture has experience of managing similar projects for State Government agencies and helping them achieve compliance as well as comply with their existing regulatory requirements. Accenture will work closely with the Commonwealth to understand the existing security standards and provide a plan to comply with the same in conjunction with Commonwealth requirements.</p> <p>Accenture's Information Security Assessment &amp; Compliance team has the expertise and experience to evaluate client's security practices and systems against the required compliance standards and regulations such as FISMA (NIST 800-53 rev4), FedRAMP, IRS-1075, CMS, Health Insurance Portability and Accountability Act (HIPAA), CJIS and others based on a defined risk profile. After each assessment, the identified findings are prioritized, and recommendations are formulated and tracked to closure.</p> <p>Based on our experience working with multiple State</p>

Ref#	Category	Question	Supplier Response
			<p>Government and commercial clients, Accenture created a Risk and Compliance framework to create a comprehensive approach to address regulatory requirements which includes updating processes, training and tools. The detailed approach would need to fine tune to Commonwealth specific requirements, but goal is creating a controls that can be reusable for multiple regulatory requirements.</p>
Q48.	Security	<p>Do you have any guidelines or best practices regarding whether the various Managed Security Services are better off being remotely hosted or on premise?</p>	<p>Managed security services have traditionally been performed on premise by personnel (client, service integrator, vendor, etc.) for various reasons including such data security or privacy, regulatory requirements, encryption requirements for network and 3rd party connectivity, cost and risk appetite. It is our experience that the following services are typically delivered on premise verses hosted remotely:</p> <p>On premise / managed security services</p> <p>Data /Systems subject regulatory controls</p> <ul style="list-style-type: none"> <li>• FISMA (NIST 800-53 rev4), FedRAMP, IRS-1075, CMS, Health Insurance Portability and Accountability Act (HIPAA), CJIS and other regulatory requirements dictate a higher level of security controls for user access, monitoring and compliance.</li> </ul> <p>Forensic Investigation – Typically requires internal resources to perform “chain of custody” activities to ensure integrity of data.</p> <p>e-Discovery – Typically performed by client resources (due to the presence of sensitive data / proprietary information) is under the direction of Legal</p>

Ref#	Category	Question	Supplier Response
			<p>Full Packet Capture – Same as above. (user information, passwords, internal IP addresses, etc.)</p> <p>Remotely hosted and managed by skilled resources via a secure, dedicated network or VPN with two-factor / SSL connection to the client network.</p> <ul style="list-style-type: none"> <li>• Security Incident Management</li> <li>• Desktop Encryption</li> <li>• Desktop Managed Host Intrusion Protection, Firewall, &amp; Antivirus</li> <li>• Server Encryption</li> <li>• Server Managed Host Intrusion Protection, Firewall, &amp; Antivirus</li> <li>• Managed Network Intrusion Protection</li> <li>• Data Loss Prevention</li> <li>• Web Content Monitoring</li> <li>• Vulnerability Scanning</li> <li>• Web URL Scan</li> <li>• Penetration Testing</li> <li>• Compliance Testing</li> <li>• Identity and Access Management</li> <li>• Application Process Whitelisting</li> <li>• WAF</li> <li>• File Level Encryption</li> <li>• Database Security Service</li> <li>• Tokenization Platform</li> <li>• Managed Encryption Platform</li> <li>• Source Code Scanning</li> </ul>
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?	Accenture would not intend to utilize any third party contractors or suppliers at this time to provide the Managed Security Services in scope.
Q50.	Scope Demarcation	VITA is interested in identifying the most efficient demarcation or bundling of these services between RFPs. For example, perhaps it	Accenture is responding to only the Security portion of the RFI and would not be able to provide

Ref#	Category	Question	Supplier Response
		<p>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.</p>	<p>additional feedback on packaging of the RFP to include some or all services. Accenture’s Managed Security Services bring clients a catalogue of end-to-end security services—processing more than 10 million security events per day and leveraging Accenture’s world-class global delivery capabilities. Accenture’s managed services enable clients to rapidly access and efficiently resource security operations with highly skilled security professionals. These professionals scan more than 52,000 client assets each year for security vulnerabilities. Accenture responds to more than 7,400 security incidents per month, and its “next gen” and “as-a-Service” projects are run on an advanced cyber defense platform that is analytics-driven, threat-centric, and industry-aligned, with SLAs prioritized against business-critical assets and business processes. Unlike commodity security services, Accenture’s state-of-the-art Security Operation Centers support the complete security incident lifecycle—identify, protect, detect, respond, and remediate—providing clients with measurably increased security effectiveness, improved security operational efficiency, and long-term business</p> <p>Please see attached our cover letter for complete details on Managed Security Service capabilities and offerings.</p>
<b>D. Financial/Managed Security</b>			
Q51.	Pricing Structure	<p>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.</p> <p>The Commonwealth will contemplate any proposed pricing structure</p>	<p>Accenture agrees with the pricing structure described in Exhibit 4.1 and 4.2, with these comments on resource units identified by VITA:</p> <p>Security Incident Management – This unit is priced by the number of FTEs, and as such, there needs to be an analysis of the time of day, number of incidents,</p>

Ref#	Category	Question	Supplier Response
		<p>along five dimensions:</p> <ol style="list-style-type: none"> <li>1. <b>Predictable:</b> 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.</li> <li>2. <b>Manageable:</b> 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.</li> <li>3. <b>Fair:</b> 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.</li> <li>4. <b>Incentives:</b> 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.</li> <li>5. <b>Flexible:</b> 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.</li> </ol>	<p>and response time for closing incidents, to verify that the staffing levels provided meet VITA’s expectations for timeliness of incident closure. Through mutual governance, there may be time when it is necessary to add staffing.</p> <p>Managed Network Intrusion Protection, Data Loss Protection, and Web Content Monitoring – These units are requested to be priced by the Bandwidth Protected. Accenture suggests that we price these units by these unit of measures:</p> <ul style="list-style-type: none"> <li>• Managed Network Intrusion Protection – Number of NIDS/NIPS devices, e.g., Firewalls, Network VPN, Network IDS/IPS, Network Anti-Spam</li> <li>• Data Loss Protection – Number of anti-virus/DLP servers</li> <li>• Web Content Monitoring - Number of Web Proxy Servers such as Akamai, Apache, Tomcat</li> </ul> <p>For these resource units where VITA is requesting the new service provide to propose resource units, Accenture suggests the following:</p> <ul style="list-style-type: none"> <li>• eDiscovery – Number of FTEs to support client’s eDiscovery program.</li> <li>• Tokenization Platform – Two resource units are suggested: 1) Number of Authentication Managers and 2) Number of Tokens.</li> <li>• Managed Encryption Platform – Number of FTEs.</li> <li>• Source Code Scanning – Two resource units are suggested: 1) Number of Applications and 2) Number of Lines of source code scanned.</li> </ul>
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	Accenture understands the Commonwealth’s concerns with billing units and how they change over time. In a recent contract, Accenture experienced this same scenario. When the contract was first developed, the client was in the midst of

Ref#	Category	Question	Supplier Response
		<p>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?</p>	<p>consolidating infrastructure due to a divestiture as well as a consolidation of infrastructure due to an acquisition occurring in parallel. Accenture worked in a pre-contract mode to develop a roadmap of how we would take over the services given this scenario. We addressed the tools technology, processes, expected scope, and the data center migrations in the roadmap. The contract was then developed, with resource units and baselines that matched the defined roadmap.</p> <p>During the first year of the contract, quarterly reviews were conducted to assess the state of the service takeover and migrations. In these reviews, the mutual governance team recognized changes in volumes and also scope. The volumetric changes were tracked monthly, then adjusted quarterly through governance as a normal course of business using an ARC/RRC methodology. Additional Resource Charges (ARCs) were used to add charges to match increased effort, whereas Reduced Resource Credits (RRCs) were used to decrease the charges to match reduced effort. The changes in scope were discussed, and in some cases, the contract adjusted to refine resource units in case of areas where it was mutually recognized that there was a mismatch between the level of effort provided by Accenture to support the client expectations, and the compensation provided to Accenture for the services.</p>
Q53.	Asset Ownership	<p>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</p>	<p>Accenture is thoughtful about owning assets on behalf of a client and would like to further discuss the Commonwealth's goals to consume services without owning assets.</p>

Ref#	Category	Question	Supplier Response
		describe your recommend financial treatment of their cost recovery for these assets.	

**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.		
C2.		
C3.		
C4.		
C5.		
C6.		
C7.		
C8.		
C9.		
C10.		