

Virginia Information Technologies Agency



COMMONWEALTH OF VIRGINIA
VIRGINIA INFORMATION TECHNOLOGIES AGENCY (VITA)
SUPPLY CHAIN MANAGEMENT DIVISION
11751 MEADOWVILLE LANE
CHESTER, VIRGINIA 23836

REQUEST FOR INFORMATION (RFI) 2017-14
FOR:
SERVER, DATA CENTER, AND SECURITY SERVICES

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

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

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

TABLE OF CONTENTS

1. Introduction.....	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	11
C. Managed Security.....	13
D. Financial/Managed Security	15
6. Feedback Regarding RFI Documents	16

1. INTRODUCTION

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

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

A. IT Infrastructure Services Program (ITISP) Overview

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

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

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

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

B. RFI Purpose

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

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

The Commonwealth has the following goals for the procurements:

Server, Storage, and Data Center Services

- Assume all existing Services for Server, Storage, Data Center LAN, and Centralized Data Center facility currently provided to the Commonwealth via the Comprehensive Infrastructure Agreement (CIA) with Northrop Grumman.
- Transition to the next generation of delivery for Server, Storage, and Data Center services to VITA and Customers, taking advantage of the ever-changing technology landscape while decreasing costs to VITA and Customers.
- Provide compute, storage, and Data Center LAN services that are flexible, rapidly provisioned, cost effective, transparent, and elastic to meet VITA and Customer needs while preserving enterprise requirements such as security and compliance management.

Managed Security Services

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

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

2. SUBMISSION LOGISTICS AND CONTACT INFORMATION

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

3. OVERVIEW OF RFI DOCUMENTS

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

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

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

4. RESPONDENT CONTACT INFORMATION

Please provide your contact information in the box below.

Contact Information	Enter your response here, enlarging the box as needed
Company Name	Symantec Corporation
Company Mailing Address	2350 Corporate Park Drive Suite 300 Herndon, VA 20171
Company Website Address	www.symantec.com
Name of Contact Person	Mike Taylor
Contact Person E-mail Address	Mike_taylor@symantec.com
Contact Person Telephone #	703-587-0223

5. QUESTIONS

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

Ref#	Category	Question	Supplier Response
A. Server/Storage Services			
Q1.	Server/Storage	The Commonwealth has upwards of 10 non-centralized Data Centers in Agency-operated buildings, primarily in the metro Richmond area. What are examples of Suppliers' best practices in managing the Servers, Storage, Firewalls, and Data Center LANs in non-centralized (Agency) facilities?	Not in Symantec Scope
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.	Not in Symantec Scope
Q3.	Data Center	What do you recommend for the length of the contract for the Data Center Facility for this type of environment?	Not in Symantec Scope
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?	Not in Symantec Scope
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?	Not in Symantec Scope
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?	Not in Symantec Scope
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?	Not in Symantec Scope
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?	Not in Symantec Scope

Ref#	Category	Question	Supplier Response
Q9.	Server/Storage	Do you see a better way to bundle or spilt the services we are requesting, in order to more effectively integrate with other towers (including MSI), and obtain more flexibility in the Commonwealth's IT environment while maintaining appropriate Governance and security?	Not in Symantec Scope
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?	Not in Symantec Scope
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?	Not in Symantec Scope
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.	Not in Symantec Scope
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)?	Not in Symantec Scope
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?	Not in Symantec Scope
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?	Not in Symantec Scope
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?	Symantec encounters this scenario often when customers are looking to displace RSA for example. Symantec's two-factor authentication solution takes advantage of the credential migration feature of the VIP Enterprise Gateway. The administrator can configure an external RADIUS authentication server called a delegation server. If a user has a registered VIP credential, the validation server will validate the

Ref#	Category	Question	Supplier Response
			supplied credentials as usual; otherwise, the validation server will attempt to authenticate the supplied credentials against the configured delegation server, in this case an RSA RADIUS server. The advantage of this scenario is that the enterprise does not have to deploy an additional VPN profile or entry point, and the experience is the same regardless whether the user uses an RSA SecurID token or a VIP token. In addition, Symantec's Access Manager allows for multiple identity providers to be used for authentication to applications.
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?	Symantec has many existing partnerships with System Integrators, Telco's and Value Added resellers where Symantec solutions (SEP, MSS, DLP, VIP, etc.) are bundled in a Managed Services environment and supporter by the prime contractor.
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)?	Dependent on the provider's ability to scale and their overall capabilities backed by existing customer reference's similar to the Commonwealth's solution requirements.
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?	Not in Symantec Scope
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?	Not in Symantec Scope
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	Symantec has migrated many customers from competitive products for MSS, SEP, DLP and many other solutions listed in the RFI. Symantec can work with MSI and/or customer directly in scheduling a

Ref#	Category	Question	Supplier Response
		regard to how the Commonwealth could migrate or transform to new Service offerings. What do you recommend for this migration plan?	transition plan for migrating solutions if considered for award. Transition Manager's, Service Manager's and Business Critical Account Manager's oversee this type of activity supported by our Remote Product Specialist and Business Critical Engineering teams.
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?	None at this time
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?	None at this time
Q24.	Enhanced Services	What would you propose as a good business case for virtualizing the desktop (offering VDI)?	From a Symantec perspective, were neutral on the subject as we can support either VDI or physical desktop environments. We see our customers evaluating VDI vs. Physical for several reasons: hardware costs, ability to track assets, hardware upgrades (RAM/bigger drive/etc.), conformity to standards, etc.
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.	Not in Symantec Scope
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?	Not in Symantec Scope
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?	Not in Symantec Scope
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,	Not in Symantec Scope

Ref#	Category	Question	Supplier Response
		disadvantages and tradeoffs of splitting the facility services out versus coupling these services with Server, Storage, Data Center LAN?	
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?	Not in Symantec Scope
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?	Not in Symantec Scope
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?	Not in Symantec Scope
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?	Not in Symantec Scope
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?	Not in Symantec Scope
Q34.	Cloud Services	When the Commonwealth buys cloud services offerings how do you propose to identify where the data and services are located?	Not in Symantec Scope
B. Financial/Server Storage			
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"> 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. 	Not in Symantec Scope

Ref#	Category	Question	Supplier Response
		<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	
Q36.	Inventory and Volume Collection	<p>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</p>	Not in Symantec Scope

Ref#	Category	Question	Supplier Response
		database support and making it a separate chargeable unit, how would the service provider collect and verify the volumes to support this chargeable unit?	
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.	Not in Symantec Scope
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?	Bundling such a vast array of services of this nature naturally lends itself to partner collaboration and integration for gap fill requirements. A caution here would be the loss of specialization to fulfill certain key categories that would require a specific expertise.
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?	Symantec's Cyber Security Services scales to fit any size organization it supports within our Managed Security Service offering globally.
Q40.	Security	Can you provide examples of comparable environments where you offer security services similar to those required by the Commonwealth?	Yes, Symantec has multiple use cases around statewide SOC consolidation both in a federated or de-centralized environments. We also work with the MS-ISAC to provide log collection within their organization.
Q41.	Security	Have you supported Managed Security services in distributed environments - both physical and virtual including on premise and off premise implementations?	Yes, Symantec has proven use cases around all distributed environments including physical and virtual.
Q42.	Security	Do you offer solutions supporting geographically diverse locations (e.g., remote location with satellite)?	Yes, Symantec has (6) Global SOC's deployed currently and monitor traffic globally on over 67M sensors.
Q43.	Security	How have you implemented solutions similar to those in the Commonwealth making use of a centralized federated environment?	Yes, Symantec has numerous use cases around SOC services within a federated environment. MS-ISAC could act as a reference if needed.

Ref#	Category	Question	Supplier Response
Q44.	Security	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?	Key challenges will be mainly around asset discovery and additional staff training. Symantec has strong expertise in providing best practice for all areas of enablement to meet this challenge without concern.
Q45.	Security	What do propose at a high level to be the key strategies and implementation elements of any typical security services solution migration?	Having a centralized integration strategy is key to any migration that involves SOC delivery and Log Collection. Working with an Integrator provides that additional level of oversight required for a successful migration. Key strategies would focus on assessment and service delivery related to onboarding of targeted assets. Once collection of logs from assets is established, the focus will transition to incident classification and understanding the activity within the VITA enterprise.
Q46.	Security	Can you recommend additional Managed Security Services that are not currently included or considered in the scope of described services?	Yes, Symantec recommends our CyberOne approach to SOC Posture with integration of Security Monitoring with Security Intelligence, Incident Response and developing a security awareness program for all levels of employees.
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?	Symantec has current certifications for our SOC offerings including PCI Compliance, ISO27001, and SSAE16. Symantec will like to discuss further requirements around regulations related to VITA specifically.
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?	Yes, Symantec has numerous successful use case where we integrate with an on-premise SIEM and our LCP for log collection and analysis (Hybrid Model) to benefit from Symantec's Big Data, Global Intelligence and our ability to cross correlate.
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?	As an OEM, Symantec will not be able to provide all the Managed Security Services requirements. Symantec will likely partner with a System Integrator, Telco or Value Added Reseller that can provide the services outside of Symantec's services offering.

Ref#	Category	Question	Supplier Response
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.	Symantec's best practices would be to separate the ops management from the log collection / incident management to allow focus on your overall SOC posture.
D. Financial/Managed Security			
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 along five dimensions:</p> <ol style="list-style-type: none"> 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. 	Symantec feels the pricing structure is in-line with the industry standards. Typically we see security products listed per Device, per Server or per User and this is currently how Symantec's licensing is structured as well.

Ref#	Category	Question	Supplier Response
		<p>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.</p>	
Q52.	Inventory and Volume Collection	<p>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?</p>	Not in Symantec Scope
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 describe your recommend financial treatment of their cost recovery for these assets.</p>	No recommendations at this time

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.		