

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 Searce, VITA Supply Chain Management (SCM)
Telephone: (804) 416-6166
E-mail Address: gregory.searce@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.....	12
D. Financial/Managed Security	20
6. Feedback Regarding RFI Documents	24

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	Deloitte & Touche LLP
Company Mailing Address	901 East Byrd Street West Tower, Suite 820 Richmond, VA 23219
Company Website Address	www.deloitte.com
Name of Contact Person	Doug Powers
Contact Person E-mail Address	dpowers@deloitte.com
Contact Person Telephone #	+1.571.471.5714

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?	
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.	
Q3.	Data Center	What do you recommend for the length of the contract for the Data Center Facility for this type of environment?	
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?	
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?	
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?	
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?	
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?	
Q9.	Server/Storage	Do you see a better way to bundle or spilt the services we are	

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?	
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?	
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.	
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)?	
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?	
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?	
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?	Our understanding of the question is that multiple providers indicates multiple solutions that are supporting IAM across the Commonwealth and its agencies. Our approach to consolidating these solutions is that we will identify the solution that covers the largest number of identities and application accounts and make that the central integrated solution. We will implement a Federated identity model with the organization where every

Ref#	Category	Question	Supplier Response
			other provider/solution will feed into this central solution as an identity provider/source. This will require a trust relationship to be established between the central solution and the provider solutions that enables the overall solution to work with a distributed identity store.
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?	
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)?	
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?	
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?	
Q21.	Migration	Suppliers will be required to provide an implantation plan to specify how they will take over responsibility for the existing environment. The Commonwealth is also interested in recommendations with regard to how the Commonwealth could migrate or transform to new Service offerings. What do you recommend for this migration plan?	
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	

Ref#	Category	Question	Supplier Response
		would you recommend these services be delivered?	
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?	
Q24.	Enhanced Services	What would you propose as a good business case for virtualizing the desktop (offering VDI)?	
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.	
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?	
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?	
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?	
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?	
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?	
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	

Ref#	Category	Question	Supplier Response
		two? What are the recommended approaches?	
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?	
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?	
Q34.	Cloud Services	When the Commonwealth buys cloud services offerings how do you propose to identify where the data and services are located?	
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"> 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 	

Ref#	Category	Question	Supplier Response
		<p>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 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>	
Q37.	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>	
C. Managed Security			

Ref#	Category	Question	Supplier Response
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?	<p>Structurally, we do not see a concern with the bundle of services requested by the Commonwealth.</p> <p>However, based on our review of the requirements, we do see a challenge with the depth and breadth of services being requested. We believe that a solution provider will need to provide the Commonwealth a solution that leverages, balances, and appropriately prices strategic thought leadership and implementable advice while also delivering the daily operational support to maintain the existing landscape.</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?	<p>We do not have a concern regarding how to scale Managed Security Services for the Commonwealth. As one of the largest cybersecurity services firms in the world, we offer a variety of strategic consulting and operational management services with tailored delivery models to suit your scope of requirements. Our practice emphasizes technical knowledge with more than 60% of our professionals possessing at least one security certification; many have more than one. We have more than 2,000 Certified Information Systems Auditor (CISA), 1,100 Certified Information Systems Security Professional (CISSP), about 120 Certified Information Privacy Professional (CIPP), and 150 Certified Information Security Manager (CISM) professionals. In addition, as discussed further in question #42, we can rapidly scale teams by leveraging our US Delivery Centers.</p> <p>However, based on the complexity of the Commonwealth's landscape we believe that transition planning will be a critical component of the initial success of this program. This will allow for your solution provider to efficiently takeover operational support activities while defining a roadmap to build</p>

Ref#	Category	Question	Supplier Response
			out and deploy more strategic initiatives for the Commonwealth.
Q40.	Security	Can you provide examples of comparable environments where you offer security services similar to those required by the Commonwealth?	<p>Our Cyber Risk Services practice has provided technology risk services in alignment with the requirements outlined by the Commonwealth for more than 20 years. Furthermore, we continue to be engaged by state agencies delivering cybersecurity services for more than 15 years; our state sector cybersecurity footprint includes serving 36 states, as well as multiple federal agencies.</p> <p>Our experienced practice is dedicated to serving various government-related entities, including cities, counties, states, colleges, universities, housing authorities, school districts, workforce agencies, welfare agencies, childcare assistance entities, and many others. While we can define our qualifications in further detail as part of our RFP response, the following accolades speak to our wealth of experience in information security services:</p> <ul style="list-style-type: none"> • Ranked as #1 globally by Gartner in Security Consulting, for the fourth consecutive year (Source: Gartner Market Insight: Security Consulting Services, Taxonomy Update 2.0, Jacqueline Heng, 04, March 2016) • Named a global leader in Cybersecurity Consulting by ALM Intelligence (Source: ALM, Cybersecurity Consulting 2015) • Named a global leader in Security Operations Consulting by ALM Intelligence (Source: ALM, Security Operations Center Consulting 2016) • Named the leader in U.S. State and Local Government Consulting by Kennedy (Source: Kennedy, United States State & Local Government Consulting 2014)

Ref#	Category	Question	Supplier Response
			Based on the needs of the Commonwealth we can draw on this wealth of experience to provide specific references to the scope and quality of our work.
Q41.	Security	Have you supported Managed Security services in distributed environments - both physical and virtual including on premise and off premise implementations?	Yes, we have experience in managing and implementing these types of complex landscapes. In fact, within Deloitte itself, we utilize similar combinations of varied and hybrid environments to meet our own security operations requirements, establishing redundant data centers and distributed operations. This allows our internal security operations center, as well as our client-facing Managed Threat Services (MTS) teams, to maintain 24x7 security monitoring despite the loss of a single facility. In addition, we have geographically dispersed technology and personnel who can provide emergency coverage during recovery from a disaster.
Q42.	Security	Do you offer solutions supporting geographically diverse locations (e.g., remote location with satellite)?	Yes, we are able to support your geographically diverse locations as well as provide services from geographically diverse locations. Deloitte currently has two US Delivery Centers (USDCs) located in Florida and Pennsylvania. We have over 1,500 resources across these two locations that can be staffed within 24-48 hours to meet your circumstances. Our USDCs leverage scale, talent, and a center-based delivery model to provide high quality, cost-effective service with standardized processes and procedures.
Q43.	Security	How have you implemented solutions similar to those in the Commonwealth making use of a centralized federated environment?	Yes, based on our history of working with state and federal agencies, our practitioners are familiar with the complexities of a federated technology landscape. We often see that this federation generally impacts the governance model of the landscape as we saw while recently developing an enterprise-wide information security framework and

Ref#	Category	Question	Supplier Response
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>implementing of a federated information security governance model at another State.</p> <p>In order to best respond to this question and support our public sector clients, Deloitte has teamed up with the National Association of State Chief Information Officers (NASCIO) in 2010, 2012, 2014, and 2016 to conduct a national cybersecurity survey. In 2016, the participants included 49 state Chief Information Security Officers (CISOs) and 186 business leaders from a broad cross-section of states.</p> <p>This NASCIO cybersecurity study documents the relative strengths and weaknesses of the security programs that protect state governments' vital systems and data, many of which are at least partially supported via a managed services provider. In addition, this study is designed to assist states with identifying potential areas of concern expressed by state CISOs and understand the tradeoffs that may be required.</p> <p>As outlined in our 2016 survey, state CISOs have indicated the following as their top three cybersecurity challenges: lack of budget, inadequate access to qualified cybersecurity professionals, and lack of documented processes. The top three cybersecurity initiatives in 2016 include training and awareness, monitoring/security operations centers (SOC), and development. We believe evaluating these challenges and opportunities and understanding how you can balance the two, is critical to the success of the managed security services effort in order to build the best information technology capabilities of the Commonwealth.</p>
Q45.	Security	<p>What do propose at a high level to be the key strategies and implementation elements of any typical security services solution</p>	<p>In order to enable the transition to managed services of security devices, we use a phased, deliverables-</p>

Ref#	Category	Question	Supplier Response
		migration?	<p>driven approach designed to maintain the controls of your environment while also establishing the new steady-state operating model. We believe the following key areas are critical in order to support a successful migration of services:</p> <ul style="list-style-type: none"> • A well-defined and accepted transition plan following a three-phased process of shadowing existing team members, sharing responsibilities, and transitioning the new vendor to the primary provider • Establishing a governance program and supporting processes to establish strategic direction, support change management, and drive decisions on initiatives • Define consistent ticket intake process in order to manage and prioritize incident requests • Gain involvement and commitment from information technology and agency leadership • Finalize the definition of service performance metrics and define the way they will be managed and reported to stakeholders
Q46.	Security	Can you recommend additional Managed Security Services that are not currently included or considered in the scope of described services?	<p>We generally recommend evaluating services that provide research and reports of Indicators of Compromise (IOC). This provides the Commonwealth with tailored intelligence to focus investigations and access to an analyst to support these follow-ups. In addition, we believe that leveraging the best practices of data analytics, data science, and high performance computing would yield significant intelligence value to the Commonwealth. Deloitte has developed a leading edge and revolutionary data analytics capability called Cyber Recon that reveals how an organization's network appears to an adversary while focusing on improving their ability to detect suspicious activity already occurring. The goal</p>

Ref#	Category	Question	Supplier Response
			is to provide actionable intelligence to allow the state to take preemptive action to address potential weaknesses while proactively diagnosing these behaviors and to derail attack campaigns.
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?	<p>The primary challenge we see for the Commonwealth with regard to regulatory requirements is to build a harmonized and broad risk and control framework that can be consistently applied to each agency while allowing for local customization to support each organization. Our State clients' agencies are often bridled with over thirty industry standards with overlapping requirements across areas such as:</p> <ul style="list-style-type: none"> • NIST Special Publication (SP) 800-53 rev4 ("Recommended Security Controls for Federal Information Systems and Organizations") • Internal Revenue Services (IRS) publication 1075 • Social Security Administration (SSA) Computer Matching Privacy Protection Act (CMPPA) • Health Information Portability and Accountability Act (HIPAA) • Health Information Technology for Economic and Clinical Health (HITECH) <p>Our recommendation is to work with a vendor that can support you with a proven public sector security risk framework to baseline your environment and use as a jumping off point to their transition plan. For example, our Deloitte framework contains more than 4,000 individual regulatory requirements mapped to more than 300 unique integrated requirements primarily driven by NIST SP800-53 rev4 but inclusive of requirements across 35 industry standards.</p>
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?	The primary characteristics we see driving the need to perform managed security services remotely versus on premise are anticipated volume and timing

Ref#	Category	Question	Supplier Response
			<p>of activities, business criticality of activities, required response time, availability of the skill-set in the marketplace and in-house, and price.</p> <p>In our experience, a blended model of capabilities is required to cost-effectively support the complexity of an information technology landscape similar to the Commonwealth's. We can strategically deploy on-premise team members to address the critical areas of your support structure who coordinate work with off-site teams. Our centralized off-site support teams allow us to scale and support variations in your demand in areas where volume is inconsistent, such as incident response, or periodic, such as audit activities. Professionals at our US Delivery Centers are available to support a variety of your managed information security services.</p>
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 part of our engagement planning process, we evaluate what opportunities we have to creatively team in order to provide our clients the capabilities needed to meet and exceed their needs. In order to support these partnerships, we have established alliances with many leaders in the global managed security services provider space. We are evaluating opportunities in the market based on the scope of requirements provided by the Commonwealth and will be able to clarify this point further as part of our RFP 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.	Based on the current delineation of security services, we see there is an overlap of responsibilities between the Multisourcing Service Integrator (MSI) with this bundle of services. This overlap can be generally characterized as shared responsibilities in identifying threats, measuring risk, defining information security requirements, and implementing controls.

Ref#	Category	Question	Supplier Response
			<p>We believe that while this type of demarcation is achievable, it underscores the need for a vendor with a strong history of teaming with other service providers. In addition, there should be a willingness as part of the MSI provider's response that components of information security services in the MSI response may potentially be better suited as primarily performed or last least equally supported by the information security provider in the following areas:</p> <ul style="list-style-type: none"> • Performance of information security planning in coordination with VITA management • Security risk and vulnerability management including platform testing and risk assessments • Security incident management • Risk prevention and mitigation through threat intelligence and network event analysis • Identity and access management (IAM)
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. 	<p><u>In order to provide the Commonwealth additional guidance to the areas highlighted as pending proposal from the new service provider within "04.1-b Exh (Pricing and Volumes Matrix - Managed Security)", we have outlined proposed units of measure for the following managed services.</u></p> <p>Source Code Scanning <u>The most accurate model would be to leverage lines of code (LOC) per application. However, we recognize that a precise calculation at times is challenging. Therefore, we also recommend a categorization effort based on estimated LOC. An example follows below:</u></p>

Ref#	Category	Question	Supplier Response								
		<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>	<table border="1" data-bbox="1272 193 1709 646"> <tr> <td data-bbox="1281 199 1465 321">Simple</td> <td data-bbox="1474 199 1701 321">500K lines of code (LOC)</td> </tr> <tr> <td data-bbox="1281 328 1465 418">Medium</td> <td data-bbox="1474 328 1701 418">500K - 1M LOC</td> </tr> <tr> <td data-bbox="1281 425 1465 516">Large</td> <td data-bbox="1474 425 1701 516">1M -2M LOC</td> </tr> <tr> <td data-bbox="1281 522 1465 646">Very Large</td> <td data-bbox="1474 522 1701 646">Up to 3.5M LOC</td> </tr> </table> <p><u>eDiscovery</u> <u>We typically propose data volume associated with eDiscovery activities</u></p> <p><u>Encryption / Tokenization</u> In our experience, the unit or metric used will depend on the type of solution chosen, along with the type of data and platforms being protected for example:</p> <ul style="list-style-type: none"> • If PII data on applications are being protected then vendors tend to price based on the number of applications that will use the encryption and decryption mechanism • If it’s only database encryption then it could be by database instances or volume of data <p>Encryption solutions at each level are closely related and it's important when implementing multiple solutions to align them together from a security coverage perspective. In our experience, successful organizations tend to create a center of excellence (COE) specific to encryption. This team or group would manage all things encryption/tokenization</p>	Simple	500K lines of code (LOC)	Medium	500K - 1M LOC	Large	1M -2M LOC	Very Large	Up to 3.5M LOC
Simple	500K lines of code (LOC)										
Medium	500K - 1M LOC										
Large	1M -2M LOC										
Very Large	Up to 3.5M LOC										

Ref#	Category	Question	Supplier Response
			<p>related. If VITA is interested in this approach, the pricing model for the different encryption solutions (e.g., Desktop encryption, server encryption, file level encryption, tokenization platform, and managed encryption platform) could be grouped together.</p> <p>For file level encryption, we often see measurements relating to the number of repositories and files that are in scope versus the number of users. For instance, if files in a SharePoint site are the target for encryption, the number of files in the SharePoint repository would be considered instead of the number of users that have access to it.</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>	<p>New units of measure have been proposed under our response in Q51.</p> <p>In regards to validating predicted volumes, such as for licensing purpose, we will work with VITA to help estimate volume. The estimation activities will depend on the service area. For example, to estimate SIEM volume we will use a list of device types and quantities to approximate sizing based on a standard SIEM sizing calculator, or if this is not available by extrapolating from data regarding raw log volume. It should be noted that this is an estimate only and where the chosen SIEM platform uses a volume-based billing model (e.g. Splunk Cloud), costs will be based on actual volumes from VITA's production environment. Services costs, such as for SOC monitoring, are not volume based and as such are generally not subject to adjustment based on changes in production environment volume.</p> <p>On at least an annual basis, we propose that the Commonwealth review service levels with their</p>

Ref#	Category	Question	Supplier Response
			provider and make mutually agreed-upon changes to project scope if needed.
Q53.	Asset Ownership	The Commonwealth consumes certain services today which are underpinned by a set of assets (servers, firewalls, etc.). The Commonwealth (or their designee) has the right to acquire these assets. The Commonwealth has a desire to consume services; rather than own assets, and envisions Supplier acquiring these assets and using them to provide services back to the commonwealth. Please describe experiences acquiring assets from an incumbent, and also describe your recommend financial treatment of their cost recovery for these assets.	In our managed security services models, we typically do not acquire assets from our clients. For example, Deloitte's SOC monitoring is based on leveraging existing VITA infrastructure accessed remotely via site-to-site VPN and does not require purchase of additional infrastructure. For this reason, we generally do not acquire assets from an incumbent MSSP vendor.

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.	0.2.1-c Exh (Description of Services) / R15 and R16	While physical security is provided as a required area within the Security Services overview section, it is unclear what the scope of requirements being requested by the Commonwealth.
C2.	02.1-c Exh (Description of Services - Security) / R5, R10, R143	Can you provide an estimate of the current landscape including approximately how many internet and external connections would be in-scope for management? How many endpoints would be included as well? How many systems and how many physical locations?
C3.	02.1-c Exh (Description of Services - Security) / R89	Based on our experience, this section is broad and will be difficult to comply with for each and every tool. Additionally, please clarify whether this section applies to all security tools.
C4.	02.1-c Exh (Description of Services - Security) / R90 and R91	Are there any pre-existing tools? If so, what are they? Is there an approved list of security tools?
C5.	02.1-c Exh (Description of Services - Security) / R102	Based on our experience, this requirement is broad and should be further clarified to determine feasibility.
C6.	02.1-c Exh (Description of Services - Security) / R103	Please clarify what "independent from Supplier services" means in this context.
C7.	02.1-c Exh (Description of Services - Security) / R146	Can you clarify the expectations on reporting requirements on collected materials?
C8.	02.1-c Exh (Description of Services - Security) / R148	Can you provide clarification on "Customer's Investigation Team"? Are these VITA personnel? Are they technical in nature?
C9.	02.1-c Exh (Description of Services - Security) / R149	In order to support estimation we would suggest adding current Log data retention periods. Also, can you clarify if these can be modified?
C10.	02.1-c Exh (Description of Services - Security) / R153	Is there a breakdown of how many of each operating system exists in the organization?
C11.	02.1-c Exh (Description of Services - Security) / R167	Does the Commonwealth intend to purchase the SIEM system and have the Supplier implement and co-manage it, or is the expectation that the Supplier will provide the SIEM?
C12.	02.1-c Exh (Description of Services - Security) / R168	We believe the ability to prevent data loss during service outages is an inherent function of the deployed SIEM, rather than the supplier's services.
C13.	02.1-c Exh (Description of Services -	Does the Commonwealth have an existing asset management system that the Supplier will be able to

Ref#	Document/Section	Supplier Commentary
	Security) / R171	access?
C14.	02.1-c Exh (Description of Services - Security) / R179	Can you clarify that the integration will be one-way connectivity, i.e. from alarm to SIEM, and that the alarm process/device generates an output alert/log in any format, including SNMP?
C15.	02.1-c Exh (Description of Services - Security) / R180	Please clarify what is meant by "other Supplier's tools and designated third parties" and the level of access that will be provided (e.g., syslog forwarding).
C16.	02.1-c Exh (Description of Services - Security) / R182	As a standard practice, we recommend that any client personnel who will be interacting directly with the SIEM undergo authorized SIEM vendor administrator training.
C17.	02.1-c Exh (Description of Services - Security) / R203	All SIEMs provide report customization, but the extent of the customization may be limited depending on the choice of platform. For example, HP ArcSight and Splunk have wide-ranging report customization functionality but this functionality is more limited for IBM QRadar and Nitro.
C18.	02.1-c Exh (Description of Services - Security) / R220	Please clarify the data retention expectations for the log repository.
C19.	02.1-c Exh (Description of Services - Security) / R226	Is there a list of approved "secure channels" or methods for secure transmission?
C20.	02.1-c Exh (Description of Services - Security) / R260	Can members of the team be part of 4.1.1 or does this have to be a dedicated team?
C21.	02.1-c Exh (Description of Services - Security) / R284	What are the criteria for classifying an incident as being "pervasive, large in scope"?
C22.	02.1-c Exh (Description of Services - Security) / R307	Is there a minimum number of exercises or test activities that need to occur?
C23.	02.1-c Exh (Description of Services - Security) / R341	Would the Commonwealth consider a service delivery model in which the Supplier's professionals monitoring the SIEM are located outside the United States but using infrastructure located entirely in the United States? No data would leave the United States.
C24.	02.1-c Exh (Description of Services - Security) / R344	Please provide additional details around anticipated scale up in terms of operational locations and network traffic.
C25.	02.1-c Exh (Description of Services - Security) / R346	Please clarify this requirement.
C26.	02.1-c Exh (Description of Services - Security) / R350	Please clarify the expectation of "resolution" for this requirement. Would "resolution" represent a handoff of the investigated alert to the Commonwealth's Security team?
C27.	02.1-c Exh (Description of Services - Security) / R381	What is the definition of a security issue? Would this include matters involving law enforcement, etc.?
C28.	02.1-c Exh (Description of Services - Security) / Sections 4.2.5, 4.2.6, 4.2.7	In our experience, the services of compliance management, vulnerability testing, and penetration are not performed within the SOC. Instead, we look at this as more general security services that would be performed across a variety of areas within your security environment. Therefore, we recommend creating a more general security services area of the requirements to address these capabilities,

Ref#	Document/Section	Supplier Commentary
C29.	02.1-c Exh (Description of Services - Security) / R519	Is the web content filtering policy required to support devices (e.g., enterprise laptops and mobile phones) outside the network? Does the Commonwealth provide such capabilities?
C30.	02.1-c Exh (Description of Services - Security) / R664	The following part of this section does not appear to related to data loss prevention: - networks, including but not limited to routers, switches, intrusion detection systems (IDS), intrusion prevention systems (IPS), firewalls, etc. for evidence of threats, and to use this information in security and threat analysis
C31.	02.1-c Exh (Description of Services - Security) / R666	Please clarify what is meant by “centralized Data Loss Prevention environment.”
C32.	02.1-c Exh (Description of Services - Security) / R667	Based on our experience, this cannot be done without the encryption key. The scope of this requirement should likely be limited to SSL traffic. Additionally, as part of later discussions during project transition, a review of the name of the proxy/proxies used will be beneficial for scoping purposes.
C33.	02.1-c Exh (Description of Services - Security) / R673, R906	Based on our experience, this should probably read: “Using only OOTB policy and signature settings is not acceptable,” as there are OOTB policies that can be effective.
C34.	02.1-c Exh (Description of Services - Security) / R681, R914, R1297	Based on our experience, this requirement is not technically feasible, as no data loss prevention system supports all devices.
C35.	02.1-c Exh (Description of Services - Security) / R682, R679-R694, R915	Please clarify whether these requirements should be specific to data at rest scanning.
C36.	02.1-c Exh (Description of Services - Security) / R898	The following part of this requirement, does not appear to related to data loss prevention: - intrusion detection systems (IDS), intrusion prevention systems (IPS), firewalls
C37.	02.1-c Exh (Description of Services - Security) / R937	Does the Commonwealth have existing/documented performance statistics or do they need to be developed by the Supplier?
C38.	02.1-c Exh (Description of Services - Security) / R937	Are there customer owned endpoints/devices in software development centers and/or operational support centers across different regions (e.g., AMRS, EMEA and APAC)?
C39.	02.1-c Exh (Description of Services - Security) / R937	Does the Commonwealth have an incident response plan as a part of the Service Management Manual in case of a malware outbreak or does it need to be developed by the Supplier?
C40.	02.1-c Exh (Description of Services - Security) / R937, R592	Is the use of open source tools planned for malware analysis?
C41.	02.1-c Exh (Description of Services - Security) / R937, R592	What is the Commonwealth’s acceptable onshore/offshore support model and required level of expertise (L1/L2/L3) for personnel supporting malware analysis?
C42.	02.1-c Exh (Description of Services - Security) / R937	Based on our experience, backup and retention related requirements needs to be defined clearly.
C43.	02.1-c Exh (Description of Services - Security) / R937	Does the Commonwealth have an existing “playbook” for troubleshooting processes?
C44.	02.1-c Exh (Description of Services - Security) / R1082	Does the Commonwealth have any specific requirements as it relates to wireless network access controls?

Ref#	Document/Section	Supplier Commentary
C45.	02.1-c Exh (Description of Services - Security) / R1082	Does the Commonwealth have IP networks enforcing access controls with regards to IP addresses? If yes, how are these access lists managed?
C46.	02.1-c Exh (Description of Services - Security) / R1082	Are the network segments defined to address the trust level of devices (e.g., jailbroken devices)?
C47.	02.1-c Exh (Description of Services - Security) / R1087	Does the system need to perform application whitelisting based on certificate, hash, services, user behavior, path, or all?
C48.	02.1-c Exh (Description of Services - Security) / R1087	Does the system need to manage custom whitelists or will they be managed by the Commonwealth?
C49.	02.1-c Exh (Description of Services - Security) / R1087	What various integration points (e.g., LDAP, Active Directory, etc.) is the solution required to support?
C50.	02.1-c Exh (Description of Services - Security) / R1119	Based on our experience with implementing and managing full disk encryption solutions, we would generally recommend considerations around the following additional requirements to those provided within this section: - The solution should support various operating systems (e.g., Windows, Mac, Unix) - If this section is meant to also cover full disk encryption for data/application servers, the solution should provide a secure key provisioning process and storage location
C51.	02.1-c Exh (Description of Services - Security) / R1140, R1161	<ul style="list-style-type: none"> • What are the different types of operating systems used for application development? • Shall there be a specific tool to be used for the scanning or vendor is expected to bring in the scanning tool? • Shall the code to be scanned be available in buildable format or non-buildable format?
C52.	02.1-c Exh (Description of Services - Security) / R1141	<ul style="list-style-type: none"> • Can the state provide an extensive list of coding languages used for web applications that will undergo the source code scanning?
C53.	02.1-c Exh (Description of Services - Security) / R1142	What are the different IDEs that are used for application development?
C54.	02.1-c Exh (Description of Services - Security) / R1144	Is there any existing framework on the basis of which the criticality can be gauged, or vendor is expected to prepare a framework first and then provide the results and recommendations?
C55.	02.1-c Exh (Description of Services - Security) / R1157, 1162, 1183	Is the vendor expected to also remediate the vulnerabilities or just track the remediation process?
C56.	02.1-c Exh (Description of Services - Security) / R1170	Is the portal already available or needed to be built from scratch?
C57.	02.1-c Exh (Description of Services - Security) / R1171	Does the client have the CVSS scores defined or the vendor needs to design a scoring system first and then gauge the scoring?
C58.	02.1-c Exh (Description of Services - Security) / R1198	Based on our experience with designing and implementing different types of encryption solutions, we would generally recommend considerations around the following additional requirements to those provided within this section:

Ref#	Document/Section	Supplier Commentary
		- Provide clarification to the functionality required by the solution (e.g., ability to preserve the format of the original data, ability to support multiple languages)
C59.	02.1-c Exh (Description of Services - Security) / R1200	<p>Definition of "systems" (e.g., databases, cloud, application, endpoint) should be provided. We recommend providing a list of systems and platforms that are in scope for the encryption solution. Different requirements may exist depending on the system or platform.</p> <p>Certain platforms and systems may not be supported by encryption solutions so it may be beneficial to vendors and the suppliers to know which systems and platforms are in scope</p>
C60.	02.1-c Exh (Description of Services - Security) / R1200	What type of data is being considered for encryption (e.g., structured or unstructured)?
C61.	02.1-c Exh (Description of Services - Security) / R1203	The current requirements for encrypting web applications only mention data in transit. In our experience, we often also see requirements around encrypting data at rest on web applications
C62.	02.1-c Exh (Description of Services - Security) / R1203	If application level encryption is being considered, is there a requirement relating to modification of application code (i.e., minimal changes required, no changes can be made)?
C63.	02.1-c Exh (Description of Services - Security) / R1242	Can any guidance and/or ranges for the typical volume of data subject to eDiscovery and/or Preservation be shared (annually, monthly etc.)?
C64.	02.1-c Exh (Description of Services - Security) / R1242	Is there a requirement or preference for an eDiscovery/Preservation solution to be deployed on or off-premise from the Commonwealth data center facilities?
C65.	02.1-c Exh (Description of Services - Security) / R1263	Is there any additional information available on the Commonwealth's implementation of strong ECC (Elliptic Curve Cryptography)?
C66.	02.1-c Exh (Description of Services - Security) / R1280	<p>Based on our experience with designing and implementing different types of tokenization solutions, we would generally recommend considerations around the following additional requirements to those provided within this section:</p> <ul style="list-style-type: none"> - For stateful type tokenization solutions (i.e., contains a token table), the token table should be stored on-premise either in a hardware security module (HSM) or a secure server - The solution should provide a tokenization system which is isolated from the data processing systems between different Production and non-Production environments - The solution should allow replacement of sensitive data with masked or redacted data in the log files <p>If format preserving encryption is being considered in the managed encryption services side then a tokenization would not be necessary. Format preserving encryption can address the same type of requirements that would be addressed by a tokenization solution.</p>
C67.	02.1-c Exh (Description of Services - Security) / R1283	Currently, the requirement specifies a reversible tokenization solution. This does not exist per standard definition of a tokenization solution. We recommend modifying the requirement to say: "2. The solution will generate random, unique tokens for each data element that are irreversible by themselves to the

Ref#	Document/Section	Supplier Commentary
		original data element."
C68.	04.1-b Exh (Pricing and Volumes Matrix - Managed Security)	In order to support estimation of service fees, we would typically request clarification on the following volumes of services: <ul data-bbox="714 305 1675 363" style="list-style-type: none"><li data-bbox="714 305 1675 337">• Forensic investigations: Are there any metrics as far as current case load?<li data-bbox="714 337 1675 363">• Incident response: Are there any metric as far as current volume of incidents