

A. Managed Security		
Q38.	Security	<p>The Commonwealth's Managed Security description of services includes all the required scope bundled for a single experienced Security Supplier. Do you see any challenges or issues with this bundled model?</p> <p>root9B does not see a challenge with the bundled model and based on our experience we would recommend the utilization of a bundled model for all managed security services. As a "Pure Play" Cybersecurity company, root9B understands the benefit of handing all security services for a customer. Through the use of a single entity for managed security services, VITA can expect a more streamlined processes overall across the program through the use of the consolidation of management and reporting of security services. The bundling of services also facilitates the integration and sharing of information from disparate Cyber activities and sensors, resulting in a more accurate and complete picture of the network's defensive state. Additionally VITA can expect a lower cost for a greater amount of services.</p>
Q39.	Security	<p>Do have any concerns or recommendations regarding how to scale Managed Security Services to organizations of the size and complexity of the Commonwealth?</p> <p>root9B recommends a solution leveraging the use of virtualization technology. This is especially important in this case considering the size and complexity of the engagement. Virtualization would help ensure that all critical services used in monitoring are properly provisioned in a High Availability cluster. Virtualization would also support Mission Assured through it's employment of computing/storage at through an alternate, off-site facility.</p> <p>Any MSS solution will be required to dynamically scale as more service and endpoints are stood up by VITA. The resources required to operate a solution of this magnitude are significant. This will require a large emphasis on storage for the retention of log files across the VITA infrastructure in addition to raw packet captures for replay activities.</p>
Q40.	Security	<p>Can you provide examples of comparable environments where you offer security services similar to those required by the Commonwealth?</p> <p>root9B's current clientele includes those from the financial, retail, utility, medical, academia, Federal, and NGO sectors that span the globe many having over 15,000+ nodes or endpoints. At all times, root9B is up-to-date on current industry standards and practices when it comes to security.</p> <p>Examples of two Clients where root9B provides MSS services are:</p> <ul style="list-style-type: none"> - Multinational Retailer - 58,000 Endpoints, ~3000 Servers, ~19,000 workstations - Large multinational NGO - 300-500 External and 4500+ Internal Endpoints
Q41.	Security	<p>Have you supported Managed Security services in distributed environments - both physical and virtual including on premise and off premise implementations?</p> <p>root9B has extensive experience to support distributed environments, to include distributed computing. We have experience providing managed security services to both physical and virtual assets, cloud-based assets in a third-party datacenter, and ensuring endpoint protection for field (telework) employees.</p>
Q42.	Security	<p>Do you offer solutions supporting geographically diverse locations (e.g., remote location with satellite)?</p> <p>root9B has supported multiple customers with internationally geographically separated environments, to include but not limited to on-premise across multiple sites over VPLS, VPN, and/or IPSec tunnels.</p>
Q43.	Security	<p>How have you implemented solutions similar to those in the Commonwealth making use of a centralized federated environment?</p> <p>root9B supports and recommends the use of a centralized federated environment whenever possible for ease of overall management and reduction in similar like services (duplication of effort). The use of Single-Sign-On throughout the VITA infrastructure, and where possible the use of two-factor authentication is highly recommended.</p>
Q44.	Security	<p>What do you consider to be the key challenges and tradeoffs for the implementation of Managed Security Services in an environment similar to the Commonwealth?</p> <p>The most challenging part in any engagement is the transitional phase. The implementation must be planned and executed with great care. This generally involves a large list of tasks that represent risk to network uptime and implementations. Once there is accurate and complete documentation, project planning will become much smoother in the initial phases of onboarding. Additionally, communication and collaboration across each sections of the program will need to be integral to the overall success of this project.</p> <p>root9B utilizes a structured execution approach for all security service transition projects. This approach provides a framework for communications, reporting, and project delivery. Some of the key project benefits we are able to offer:</p> <ul style="list-style-type: none"> • Risk is managed more effectively because the project is properly defined within your business environment and threats are clearly identified and mitigation plans developed. • Productivity is increased through a clear definition of roles, responsibilities and deliverables. This gives a faster start up, less rework and more productive time in the project. • Communication is easier and clearer. <p>To transition your security service delivery, whether directly from your internal IT organization or from another service provider, is a critical effort with potentially significant impact on your operations. To manage the risks, root9B takes a stringent, unwavering approach to transitions, executing them in a non-disruptive and responsive manner, always geared to managing any issues that might arise.</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 migration?</p> <p>The largest element during the implementation process will be the planning process as it involves deciding what devices are needed, determining device locations within your architecture and establishing proper configurations. A project manager will need to be assigned to provide a single contact to coordinate all teams, VITA, Administrators, Engineers, etc. In our experience, this provides the optimal solution to provide the most efficient service</p>
Q46.	Security	<p>Can you recommend additional Managed Security Services that are not currently included or considered in the scope of described services?</p> <p>Based on the MSS strategy root9B has applied to its customers, we would recommend incorporating active adversary pursuit, or HUNT services. Additionally, VITA has identified Distributed Denial of Service (DDoS) as being included in a Web Application Firewall solution, but the prevention of such attacks are best suited for dedicated appliances. root9B would recommend putting DDoS under a separate solution.</p>
Q47.	Security	<p>Based in your experience, what are the key challenges with regard to the regulatory requirements included in the scope of services? Do you have any recommendations based on your experience?</p> <p>The key challenges in regard to regulatory requirements and compliance is keeping up to date with latest changes and standards. root9B will work with VITA to ensure full regulatory compliance without losing sight of the overall goal: protection of your critical information assets.</p>
Q48.	Security	<p>Do you have any guidelines or best practices regarding whether the various Managed Security Services are better off being remotely hosted or on premise?</p> <p>While certain solutions are best kept on-premise, others can be best suited in a cloud based (remotely hosted) environment to reduce the large capital investment required associated with hosting large data sets. root9B would recommend a hybrid approach and would work with VITA on identifying which Security Services are best suited for each remote hosting scenario.</p>
Q49.	Security	<p>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?</p> <p>root9B has organized its cyber services accordingly and can ensure all the necessary skillsets required to perform these tasks can be met.</p>
Q50.	Scope Demarcation	<p>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.</p> <p>To best provide any feedback, root9B would need to better understand the expected scope and timelines for each RFP. In general, however, root9B recommends that MSS be provided under a separate RFP. VITA will be best served with a specialized security services vendor that is wholly focussed on providing security solutions versus a vendor that focuses on IT, Datacenter, and Security activities.</p>

<p>Q51.</p>	<p>Pricing Structure</p> <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. The Commonwealth will contemplate any proposed pricing structure along five dimensions: 1. Predictable: To the greatest extent possible, customers should be able to forecast charges ahead of time; changes in pricing that occur over time should not be a surprise. 2. Manageable: The pricing should not be so complex that it is needlessly difficult to administer. If quantities of work or equipment in the environment must be measured, then those quantities should be as easy and transparent as possible to measure. 3. Fair: The service pricing must be a reasonable proxy for a services provider's underlying costs and should adequately recover those costs. Additionally, to the extent possible, the party that causes any incremental cost should bear that cost. 4. Incentives: All pricing structures will incentivize certain behaviors and discourage others. The goals of the sourcing program must be kept in mind when considering the behaviors that might be driven by a pricing structure. For example, a goal to encourage server consolidation might include reduced cost at a centralized data center. 5. Flexible: As consumption moves up and down, the charges should also adjust. Technology is an evolving industry, and the ability to turn down an old service to turn up a new service is one</p>	<p>One pricing model may not be ideal for all MSS services and instead may need to be based on overall services and type of devices supported. A number of the devices associated with Sections 2.2, 2.3, and 4.2, can accurately be measured by capacity of bandwidth. While bandwidth usage as a measurement is ideal for Web Content Filtering and DDoS Appliances, this may not be the case for all VITA devices. Other types of devices (Firewall, IDS/IPS, UTM, etc...), however, should be identified separately and be measured on a per device (vs bandwidth projections). Depending on the solution for DLP services, pricing may need to be modified to reflect and distinguish between endpoint and bandwidth pricing. Note that root9B offers pricing based on this combined bandwidth and security nodes model. To ensure that our pricing accurately reflects the Client's changing network configurations, we revise our pricing based on current security device inventory and offer quarterly "true ups" .</p>
<p>Q52.</p>	<p>Inventory and Volume Collection</p> <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>Through the use of a SIEM, root9B can determine the volume of devices, device type and cross-correlate the services being offered to VITA for Managed Security Services. A dashboard and reports could be provided to VITA to assess each asset type based on agreed upon unit of measure and provide the necessary metrics. A period of True-Up/Down could also be established on the contract to reflect any required changes towards changes on inventory and volume throughout the live on the contract.</p>
<p>Q53.</p>	<p>Asset Ownership</p> <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>	<p>root9B is positioned as a reseller for various products, however, once these assets are installed within the customers' space they become the property (and responsibility) of the Client. The expense and outlay associated with a technical refresh for a Client's entire enterprise will likely preclude any small businesses from priming a VITA contract.</p>