Exhibit 2.1

Description of Services

Modification 26

VA-180112-ATOS

COMMONWEALTH OF VIRGINIA
VIRGINIA IT AGENCY (VITA)
SUPPLIER STRATEGY AND PERFORMANCE DIVISION

7325 Beaufont Springs Drive
Richmond, VA 23225

Table of Contents

1.0 Introduction

This **Exhibit 2.1 (Description of Services)** sets forth the Services that Supplier will provide, as of the Commencement Date unless otherwise specified. Further, this **Exhibit 2.1 (Description of Services**) sets forth the processes and systems that the Supplier will provide and describes the Supplier's obligations to work with other VITA suppliers in the Managed Environment to deliver integrated end-to-end Services to Customers.

This document is separated into service areas indicating where each security service will be implemented. There are duplicate areas or requirements in some service areas that may be satisfied with a single solution. The requirements are repeated in different service areas in case multiple solutions are utilized to more effectively deliver the Services. Each service area is intended to be an integrated service consumable by VITA and Customers.

The requirements that will be included as part of the Services are classified into the following categories:

1. **Information Security Program -** This section includes information about the general information security program requirements that all suppliers including the security services Supplier must satisfy. The requirements include components of the security program in addition to specific documentation that should be included. Additionally, this section includes some of the requirements for integrating with suppliers in the environment. The security Supplier will need to collect, monitor, and integrate multiple systems and data sources. Supplier is also required to provide the cross-functional services as set forth in **Exhibit 2.2 (Description of Services – Cross-Functional)**, which are common to all Service Tower Suppliers and support integration in the Managed Environment.
2. **Security Services** – This section includes the detailed requirements for the following security related areas:
    a. **Threat Management –** Threat management includes the integration and monitoring of data from all components of the Managed Environment for analysis and review of the environment. The data is reviewed for security issues and when a compromise of a security control occurs there are resources that will remediate the situation and restore services back to functioning.
    b. **Perimeter Security -** This section includes requirements pertaining to security controls between the internet and other external connections. These security controls are designed to protect the environment from threats originating outside of the Customer networks and Managed Environment.
    c. **Internal Network Security** - This section includes the security requirements for protecting the internal network which includes communication between devices within the Customer networks and the Managed Environment.

d. **End Point Security** - This section addresses requirements for end points in the Managed Environment. These controls may extend to any device including but not limited to servers, desktop, mobile devices, etc. More than one platform is used in providing end point security.
e. **Application Security** - Application security controls focus on applying security measures that impact applications. The controls are intended to provide additional security for circumstances when the security controls are needed as well as when there are compensating controls required.
f. **Data Security** - Data security includes security controls that are intended to protect Commonwealth data. Data may traverse or be stored both within and outside the Managed Environment. The controls included in this section focus on protecting the data itself with controls such as encryption.

3. **Physical Security** - Physical security controls are intended to protect the facilities where the hardware, systems, and other tangible components of the Managed Environment are located.

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1.	**2.0 Information Security Program Requirements**		
R2.	**2.1 Information Security Program**		
R3.	*This section includes information about the general information security program requirements that all suppliers including the security services Supplier must satisfy. The requirements include components of the security program in addition to specific documentation that should be included. Additionally, this section includes some of the requirements for integrating with suppliers in the environment. Supplier will be responsible for operating within the parameters of Customer's information security policies and standards.* *Supplier's responsibilities include:*		
R4.	1. Adhere to the current safety and security policies, rules, procedures and regulations established by the Commonwealth and VITA, VITA Rules, and each Customer with respect to such Customer's data and facilities (including, for example, SEC501-09, SEC525-02, SEC514-04, SEC511, SEC511).	Y	
R5.	2. Develop, implement and maintain standards, objectives, processes and procedures to maintain compliance within the scope of the Services which support Customer's information security policies and standards.	Y	
R6.	**2.2 Information Security Practices and Processes**		
R7.	*Supplier will be responsible for providing information security practices and processes to protect the Customer Environment and Customer Data.* *Supplier's responsibilities include:*		
R8.	1. Ensure that Supplier's security processes comply with Customer's security requirements and VITA Rules.	Y	
R9.	2. Notify designated parties regarding risk as identified in the Service Management Manual.	Y	
R10.	3. Provide Services that support Commonwealth business needs, security, technical requirements, and End-User requirements.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R11.	4. Communicate Customer's security requirements in detail to Customer and End Users (including Customer's departments and groups) and Supplier's.	Y	
R12.	5. Identify security risks and vulnerabilities, and recommend improvement opportunities for reducing the impact of such risks and vulnerabilities as they are identified.	Y	
R13.	6. Assess and recommend improvements via a monthly report based on security vulnerability and risk assessments.	Y	
R14.	7. Implement such recommendations that are approved by Customer or VITA.	Y	
R15.	8. Recommend changes to Customer's security requirements in order to incorporate industry best practices, infrastructure roadmap changes, and document the evolution of such changes and practices in a quarterly report.	Y	
R16.	9. Deploy security processes to enable the effective monitoring and reporting of the services in the Customer Environment through the appropriate deployment of the relevant tools and procedures, and where such security processes do not exist, designing processes that are in compliance with security requirements.	Y	
R17.	10. Comply with VITA and Commonwealth policies, VITA Rules, standards and regulations for information, Systems, personnel, physical and technical security.	Y	
R18.	11. Conform to changes in laws, regulations and policies.	Y	
R19.	12. Participate in coordination of all changes to the IT infrastructure.	Y	
R20.	13. Provide timely creation, updating, maintenance and provision of all appropriate project plans, project time and cost estimates, technical specifications, management documentation and management reporting in open industry standard portable format, for all projects and service activities.	Y	
R21.	14. Coordinate Service delivery with Suppliers as well as other support groups with Customers, VITA, and all appropriate third-parties.	Y	
R22.	15. Provide for VITA identified immediate support services.	Y	
R23.	16. Provide fraud prevention, detection and reporting.	Y	
R24.	17. Provide infrastructure, security planning and analysis, installation and upgrade recommendations.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R25.	18. Continuously monitor security trends through independent research; document and report on products and services with potential use for the Commonwealth.	Y	
R26.	19. Perform feasibility studies and evaluations for the implementation of new security technologies that meet Commonwealth business needs and meet cost, performance and quality objectives.	Y	
R27.	20. Participate in technical and business planning sessions to establish security standards, establish architecture and identify initiatives.	Y	
R28.	21. Conduct technical reviews and provide recommendations for improvements to the infrastructure that increase efficiency and effectiveness of security and reduce costs in accordance with planning and analysis policies and procedures.	Y	
R29.	22. Recommend potential improvements to application security architecture and infrastructure service architecture.	Y	
R30.	23. Perform application security review to ensure compliance with infrastructure requirements.	Y	
R31.	24. Ensure requirements meet VITA and Commonwealth security policies and standards.	Y	
R32.	25. Develop and document technical design plans and environment configuration based on VITA and Commonwealth security requirements.	Y	
R33.	26. Conduct security testing for all new, changed, and/or upgraded equipment, Networks, Software and Services to include unit, System, vulnerability, integration and regression testing.	Y	
R34.	27. Evaluate all new and upgraded service components and services for compliance with VITA and Commonwealth security policies, regulations and procedures.	Y	
R35.	**2.2.1 Security Awareness and Training**		
R36.	*Supplier will be responsible for facilitating awareness of security requirements and best-practices within Customer user communities.* *Supplier's responsibilities include:*		
R37.	1. Implement and maintain processes and procedures, and provide communications, that are intended to increase security and privacy awareness, including:	Y	
R38.	1.1. Communications regarding changes to security requirements	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R39.	1.2. Urgent communications on high-risk threats	Y	
R40.	1.3. Routine communications on general awareness topics	Y	
R41.	2. Promote security awareness through a role based training program that includes creation and delivery; measure and report on such program's effectiveness.	Y	
R42.	3. Obtain and review industry-recognized information sources regarding security, provide information to Customer, and, on a quarterly basis, recommend, in the form of a report, security risk reduction actions and opportunities based on review of such information.	Y	
R43.	4. Conduct an awareness campaign to cover Customer privacy and security topics and standards. This campaign should include simulated social engineering attacks.	Y	
R44.	5. Actively participate in industry standard security forums and End-User groups to remain up to date with current security trends, threats, common exploits and security policies and procedures.	Y	
R45.	**2.2.2 Governance, Risk and Compliance Tracking**		
R46.	*The Supplier will be responsible for maintaining security governance, risk and compliance-related information.* *Supplier's responsibilities include:*		
R47.	1. Provide integration for the software, hardware, and Application framework necessary for automation of the associated processes.	Y	
R48.	2. Educate and train Supplier Personnel on the proper use of the governance, risk and compliance Tool(s).	Y	
R49.	3. Integrate the governance, risk and compliance tool(s) with the asset compliance data repository or application (i.e. MSI provided asset management system). Two-way data exchange is required with the asset compliance system.	Y	
R50.	4. Provide the completed initial assessment information to Customer for the determination of the data risk rating for the vendor supplied service being assessed.	Y	
R51.	5. Provide security control compliance data. The security controls are rated by the compliance tool(s) and include the identification of any gaps based on the current Customer information security policies.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R52.	6. Manage the remediation of compliance gaps and track the remediation plan to completion in the governance, risk and compliance Tool(s).	Y	
R53.	7. Integrate the governance, risk and compliance Tool(s) with source data in order to track and report the status of all systems with exceptions requested, needed, or identified as specified in the Service Management Manual.	Y	
R54.	8. Manage policy exceptions based on the policy requirements and consume exception information from the governance risk and compliance Tool(s).	Y	
R55.	9. Maintain a repository of projects and other initiatives and their associated security risks and compliance issues.	Y	
R56.	10. Provide new governance, risk and compliance Tool use cases for the automation of risk and compliance processes as needed.	Y	
R57.	11. Gather requirements and document the use cases for all new functions.	Y	
R58.	12. Assist with design, development and implementation of the use case in the governance, risk and compliance Tool(s) including the integration with other source systems as needed to automate the use case.	Y	
R59.	13. Assist with the implementation of the required workflow, notifications, dashboards and reporting as defined by the use case specification.	Y	
R60.	14. Create data exports of security compliance information as required in order to feed data to other security Applications. Develop an automated and secure file transport process for the data extracted from the governance, risk and compliance Tool.	Y	
R61.	**2.3 Service Integration**		
R62.	**2.3.1 Systems and Tools**		
R63.	*For many of the functions described in this **Exhibit 2.1 (Description of Services - Managed Security)**, Supplier is required to provide systems and tools or use a system provided by Customers.* *Supplier's responsibilities include:*		
R64.	1. Limit access to security Tools to the agreed levels (e.g. by business unit) for the type of designated users who require access to the system.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R65.	2. Provide access to security Tools to Customers, business units of Customers, and authorized Third Party Vendors, and any other parties identified in the Service Management Manual which access will include all appropriate and required licenses and interfaces.	Y	
R66.	3. Provide for granting additional access in support of other designated Third Parties (e.g. auditing organizations) upon request.	Y	
R67.	4. Support activities to verify security Tools contents and correctness of the information contained therein by VITA, Customers and other designated Third Parties (e.g. auditing organizations).	Y	
R68.	5. Educate and train Supplier and designated personnel in current information security trends and the use of security tools used in the environment or anticipated to be used in the environment.	Y	
R69.	6. Recommend new security Tools to be included as part of the Services (including any Equipment, Software products, and infrastructure services).	Y	
R70.	7. Provide, in the program-wide dashboard, monthly reports on the status of and maintenance activities for the security Tools.	Y	
R71.	**2.3.2 Supplier Security Tools**		
R72.	*Supplier will be responsible for providing any Tools necessary for the execution of the Services, including the Supplier-provided security Tools.* *Supplier's responsibilities include:*		
R73.	1. Provide, deploy, install, implement, configure, maintain and administer VITA/Customer-approved security Tools, including security Tools that support ITIL-based processes, and those tools identified in the Service Management Manual and accordance with VITA Rules.	Y	
R74.	2. Provide access to a raw feed as well as to monitoring and reporting interfaces for the security Tools dedicated to Customer and customer identified entities.	Y	
R75.	3. Subject to the Customer's prior written approval, leverage new security Tools that would improve Customer's business processes.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R76.	4. Maintain the technical and functional specifications and requirements for the Supplier-provided security Tools and any interfaces.	Y	
R77.	5. Secure security tools and its data such that the data is clearly separated from all other customers of Supplier and the customers of Supplier's subcontractors or other vendors.	Y	
R78.	6. Partition Customer information in management and reporting, such that Customers cannot inappropriately access the information of another Customer.	Y	
R79.	7. Provide Supplier personnel, Customers, business units of Customers, authorized Third Party Vendors, and other parties identified in the Service Management Manual with appropriate training in using security tools.	Y	
R80.	8. Grant access to the supporting database(s) of security tools to Customers, and entities designated by Customers.	Y	
R81.	9. Allow Customers to monitor, view and download such database(s) on an ongoing basis.	Y	
R82.	10. Provide extract, load, and transform capabilities for the supporting database(s) of security tools.	Y	
R83.	11. System(s) will be accessible by secure web browser (i.e. HTTPS), unless otherwise approved by VITA.	Y	
R84.	12. Maintain separation of duties between administrator and security personnel.	Y	
R85.	13. Provide a mechanism for centrally collecting security data that remains independent from Supplier services.	Y	
R86.	14. All tools must integrate into the existing authentication services.	Y	
R87.	**2.3.3 Patch Management**		
R88.	*For Systems under management, Supplier will be responsible for patch deployment and control of the software and devices under management. Supplier will be responsible for participating in Customer change management processes to deploy patches on a regular basis. Supplier's responsibilities include:*		
R89.	1. Participate in Customer's patch rating process.	Y	
R90.	2. Provide reports on the status of patching every 30 days and upon request.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R91.	3. Patch all equipment, systems, software, and other devices that are part of infrastructure services. Use the approved central software deployment tool and deploy patches to servers and clients per Customer's policies and VITA Rules.	Y	
R92.	4. Provide results of patch management piloting process to the impacted Customers and VITA.	Y	
R93.	5. In the event that the patch process disrupts Customer operations the Supplier will roll back the changes made.	Y	
R94.	6. Apply patches to devices within the timeframe guidelines in accordance with Customer's security policies and the Service Management Manual.	Y	
R95.	7. Communicate with and/or alert the Customer IT Security team when patches are not installed within the designated timeframe.	Y	
R96.	8. Integrate and have the ability to export patch data associated will all Customer devices.	Y	
R97.	9. Provide an analysis of security patches impacting the environment on a weekly basis including advisory actions and recommended patch time frames.	Y	
R98.	**2.3.4 Reporting**		
R99.	*Reporting functions and specific operational reports as defined in **Exhibit 3 (Service Levels and Reporting)**.* *Supplier's responsibilities include:*		
R100.	1. Provide integration into the real-time security dashboard and monthly reports in the Security Dashboard.	Y	
R101.	2. Retain all reporting information online for 90 days, archived for 1 year, and available as a 3-year trend.	Y	
R102.	**2.3.5 Security Dashboard**		
R103.	*Supplier will provide an online reporting facility for all security-related information, including System compliance, security Tool deployment progress, Malware trends, (the "Security Dashboard").* *The security dashboard will be able to support providing individual agency/customer views as well as a program view.* *Supplier's responsibilities include:*		

Ref#	Requirement	Comply (Y/N)	Supplier Response
R104.	1. Provide near real-time health dashboards for any Systems managed by Supplier highlighting status of health metrics as defined by Customer.	Y	
R105.	2. Provide reporting monthly, quarterly and annually in the Security Dashboard on the deployment of Tools and procedures to the Customer Environment.	Y	
R106.	3. Provide Customer user access to dashboards as requested.	Y	
R107.	4. Provide real time access to collected log information from software, equipment, network, infrastructure services, and any sources identified in the Service Management Manual in compliance with VITA Rules.	Y	
R108.	5. Security dashboard will include alerts as specified in the Service Management Manual.	Y	
R109.	6. Provide training for the dashboard to Suppliers, Customers, and designated users.	Y	
R110.	7. Include VITA's, Customers' and Supplier's threat trend alerts on the security dashboard.	Y	
R111.	8. Provide access to threat data as defined in the Service Management Manual.	Y	
R112.	9. Provide access to security incident information as defined in the Service Management Manual.	Y	
R113.	10. Maintain 3 years' worth of trend data for security dashboard information.	Y	
R114.	11. Maintain 90 days of collected information online and 1 year of information that is available in near time.	Y	
R115.	12. Include reference to the most recent security advisory list for the software, equipment, systems, and infrastructure in use by the Customer.	Y	
R116.	13. Provide information about the compliance requirements for patching status, security baseline requirements, and any other compliance requirements identified in the Service Management Manual.	Y	
R117.	14. Integrate where identified with the program dashboard.	Y	
R118.	15. Provide customers with the ability to run ad hoc reports and export data.	Y	
R119.	**3.0 Security Requirements**		
R120.	**3.1 Threat Management**		

Ref#	Requirement	Comply (Y/N)	Supplier Response
R121.	*Threat management includes the integration and monitoring of data from all components of the Managed Environment for analysis and review of the environment. The data is reviewed for security issues and when a compromise of a security control occurs there are resources that will remediate the situation and restore services back to functioning.*		
R122.	**3.1.1 Digital Forensics Investigation**		
R123.	*This section identifies requirements that the Supplier will include in the recovery and investigation of material found in digital devices as part of security incident response. Supplier's responsibilities include:*		
R124.	1. Provide digital forensics services to collect, examine, investigate, and report on access and use of VITA and Customer computer systems and designated parties.	Y	
R125.	2. Document and manage processes that provide a chain of custody for all materials collected.	Y	
R126.	2.1. Provide controls that prevent and manage change in collected materials.	Y	
R127.	2.2. Uniquely track and report on collected materials.	Y	
R128.	3. Provide reverse engineering and systems analysis capabilities.	Y	
R129.	4. Provide assistance to VITA or Customer's Investigation Team with any investigations (e.g., employee misconduct, fraud, embezzlement).	Y	
R130.	5. Provide evidence acquisition services, including log data collection.	Y	
R131.	6. Ensure that all collected evidence adheres to documented chain of custody procedures and remains forensically sound throughout the process.	Y	
R132.	7. Attempt to salvage deleted or otherwise unrecoverable data from a variety of media and data types including server and Workstation hard disks, backup media, optical media, email information stores, smartphones, tablet computers, and .pst files, as applicable.	Y	
R133.	7.1. Supported drive interfaces will include SATA, IDE, SAS, SCSI, USB and NAND (flash) memory.	Y	
R134.	7.2. Supported operating systems may include Windows, MAC OS X, Linux, UNIX, Solaris, Android, IOS, Mainframe, etc.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R135.	8. Maintain the capability, lab environment, Tools, and skills to reverse engineer Malware to provide a detailed analysis of attack vectors.	Y	
R136.	9. Analyze information collected:	Y	
R137.	9.1. Rebuild webpages and display webpages in their original format as they were seen by the user.	Y	
R138.	9.2. Identify and report geo-location data indicating physical locations.	Y	
R139.	9.3. Perform keyword searches, filter and bookmark important evidence discovered.	Y	
R140.	9.4. Identify the date and time when information was created, accessed, modified, and deleted.	Y	
R141.	9.5. Identify the user id or other identifying information, as available, of individuals who created, accessed, modified, and deleted the information.	Y	
R142.	9.6. Provide an activity timeline of notable events associated with the investigation and/or incident.	Y	
R143.	10. Report on the results of digital forensics investigations in a format identified in the Service Management Manual.	Y	
R144.	11. Coordinate with U.S. Computer Emergency Response Team (US-CERT) or other VITA identified third party entities as directed by VITA.	Y	
R145.	12. Present a timeline view showing artifacts graphed in a chronological sequence to observe overall activity patterns, and the ability to drill-down to isolate artifacts from a specific time period.	Y	
R146.	**3.1.2 SIEM**		
R147.	*Supplier will provide security incident and event management (SIEM) services as a solution that provides real-time analysis of security alerts generated by systems and applications in a manner specified within the Service Management Manual.* *Supplier's responsibilities include:*		
R148.	1. Install, configure, and manage hardware and software required for the purposes of event transmission, collection, correlation, separation of duties, and reporting in SIEM and log management systems in accordance with VITA Rules and Service Management Manual.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R149.	2. Employ appropriate methods to ensure that service outages do not result in a loss of event data in the collection or storage processes.	Y	
R150.	3. Ensure that all SIEM data will be stored in accordance with VITA Rules, regulatory requirements, and the Service Management Manual.	Y	
R151.	4. Develop and maintain an inventory of systems and applications with alerts being collected and analyzed.	Y	
R152.	5. The service and system inventory should include: Application names, service names, versions, service descriptions, data collection method, and data collection component as well as event description documentation.	Y	
R153.	6. Make inventory information available electronically to VITA and Customer personnel.	Y	
R154.	7. Participate in the Security Incident response processes to provide necessary resources to support resolving Security Incidents.	Y	
R155.	8. Perform regular SIEM and log management system and component performance assessments and tuning exercises.	Y	
R156.	9. Establish a process to proactively monitor key SIEM components' performance.	Y	
R157.	10. Periodically, at least semi-annually or as specified in the Service Management Manual, perform a capacity analysis for all components that use any infrastructure resources (i.e. WAN bandwidth, storage, process, etc.), for the purpose of business impact mitigation.	Y	
R158.	11. Provide designated users access to real-time and historical event feeds, rule logic, report components, filters, data lists, variables, queries for validation and investigation, and any other areas specified in the Service Management Manual or VITA Rules.	Y	
R159.	12. Provide designated users with the ability to develop and apply complex query logic to real-time and historical data.	Y	
R160.	13. Ensure that SIEM content is capable of integration with operations alarm processing (e.g., alarm boards) using real-time network protocols such as SNMP.	Y	
R161.	14. Establish mechanisms so that SIEM content will trigger specified alerts, and report on requested content including other Supplier's tools and designated third parties.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R162.	15. Provide mechanisms so that any real-time alarms, reports and email notifications may be directed at more than one user. Designated recipients may be individual agents or a larger distribution list.	Y	
R163.	16. Provide training on how to interact and use the SIEM once installation is complete and after any upgrades or changes.	Y	
R164.	17. Provide custom content development, custom content tuning, real time alarming, escalation, and proactive content development in response to threats. Services which require monitoring include:	Y	
R165.	17.1. Host based intrusion detection/prevention systems	Y	
R166.	17.2. Network intrusion detection/prevention systems	Y	
R167.	17.3. Firewalls	Y	
R168.	17.4.		
R169.	17.5. Workstations (e.g., operating system security logs, firewalls and security agents)	Y	
R170.	17.6. Network devices such as routers, managed switches, traffic management switches, application layer switches, and wireless access points	Y	
R171.	17.7. Server	Y	
R172.	17.8. Access control, authorization services such as proxies, reverse proxies, TACACS, Microsoft Active Directory, LDAP, multi-factor authentication systems and single-sign-on systems	Y	
R173.	17.9. Applications	Y	
R174.	17.10. Any other sources or services specified in the Service Management Manual	Y	
R175.	18. Ensure that the SIEM solution is capable to produce the following types of content:	Y	
R176.	18.1. Customizable real-time rules, based on complex logic.	Y	
R177.	18.2. Customizable, scheduled and ad-hoc reporting based on complex queries with complex logic.	Y	
R178.	18.3. Customizable page and content layout.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R179.	18.4. Trending data based on source log values. Trending will be used in both reporting and proactive anomaly detection and alerting.	Y	
R180.	18.5. Data values that result from custom real-time rules used for future reporting or secondary rules.	Y	
R181.	18.6. Filter logic will be applied to existing rules, reports, event feeds sent to the SIEM for capacity management, and any other areas specified in the Service Management Manual.	Y	
R182.	19. Normalize log values for all supported log feeds into a common set of fields for all feeds. The normalization and uniform nature of fields is the essential core of an effective SIEM. Log feeds will have common fields as specified in VITA Rules and as identified in the Service Management Manual.	Y	
R183.	20. Ensure that the SIEM solution is capable of implementing complex, layered, Boolean logic across multiple normalized fields and log types.	Y	
R184.	21. Make template customization available to define the visual layout and structure of reports as needed.	Y	
R185.	22. Provide field customizable templates for email notifications to be sent to designated individuals.	Y	
R186.	23. Provide for complex filtering capability on logs and event collectors to reduce undesired data collection.	Y	
R187.	24. Provide for aggregation on logs and event collectors for event storage de-duplication.	Y	
R188.	25. Ensure the ability to detect changes to audit records created by the solution (i.e., data hashing).	Y	
R189.	26. Classify and prioritize collected data for the purpose of applying access control and retention policies.	Y	
R190.	27. Provide the ability to apply retention policies by data type and source.	Y	
R191.	28. Provide role-based data access control; restrict data view by role.	Y	
R192.	29. Provide mechanisms for filtering rules and report creation.	Y	
R193.	29.1. Obtain approvals for all filters implemented.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R194.	29.2. Document the justification for all filters implemented for rules and reports related to security content.	Y	
R195.	30. Perform on-going alarms review and tuning on the schedule specified in the Service Management Manual. Implement alarms and content changes based on review results.	Y	
R196.	31. Provide processes and support quality assurance tests (e.g., penetration tests, generation of distributed denial of service activities, generation of security alarms) of the security processes and Security Incident response functions by generating Security Events and monitoring to determine if the appropriate action is taken at each step of the process.	Y	
R197.	32. Provide an operational SIEM report to summarize and provide data as specified in the Service Management Manual or on demand from VITA.	Y	
R198.	33. All servers and infrastructure devices will be logged to the SIEM.	Y	
R199.	34. Solution must be available for use by individual Customers and other towers as directed by VITA.	Y	
R200.	35. Solution must be able to export events into common file formats such as XML, CSV, etc.	Y	
R201.	36. Maintain a repository of collected logs that is accessible by Customers for consumption or review.	Y	
R202.	**3.1.3 Security Incident Response**		
R203.	*Security Incident Response develops and executes well understood and predictable responses to damaging events, computer intrusions, security compromises and inadvertent data disclosure or loss. As part of Security Incident Response, Supplier will provide the necessary resources to support VITA, Suppliers and Customers in preparing for and resolving Security Incidents, that are reported by any source including the MSI provided service desk, the customer and/or self-reporting by the Supplier.* *Supplier's responsibilities include:*		
R204.	1. Initiate incident response as directed by VITA and in accordance with requirements included in the Service Management Manual and VITA Rules.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R205.	2. Provide a technical team of subject matter experts on general security practices and the technology utilized in the environment to be available at all times to respond to Security Incidents.	Y	
R206.	3. Track all security incidents in accordance with requirements ensuring that security incidents are appropriately segregated from Service Desk.	Y	
R207.	4. Provide a dedicated investigative group, who will serve as a security incident response point of contact. The group will respond to any security incident related requests including a phone 'hotline', and will contribute to the delivery of emergency Incident response services.	Y	
R208.	5. Provide any logs, alerts, and event information required to respond to security incidents through secure channels.	Y	
R209.	6. Coordinate investigation activities in conjunction with VITA and Customers to maintain the data integrity of any asset which may be needed for evidence or forensic review.	Y	
R210.	7. Securely collect, capture, and retain any data or hardware deemed necessary to assist with Security Incident response using a forensically appropriate process, including logs, disk drives, files, servers, work stations, and other items which may be of evidentiary value.	Y	
R211.	8. Provide and execute an enforceable chain of custody process for all Security Incidents, such that evidence integrity is maintained for any items (physical or logical) relating to the incident response investigation.	Y	
R212.	9. Assist in validating and determining the impact and scope of each suspected security incident.	Y	
R213.	10. Identify the initial point of entry into the system, the source of the intrusion, the tools and methods employed by the intruders, and any data compromised, as well as a list of all other systems, Applications, or third-parties potentially compromised.	Y	
R214.	11. Determine, document, and report root cause of Security Incidents as defined in the Service Management Manual.	Y	
R215.	12. Conduct, or participate in as requested, event calls for the purposes of escalating and resolving a Security Incidents.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R216.	13. Work with VITA and Customers in the restoration of the Customer environment in accordance with VITA Rules.	Y	
R217.	14. Refer requests for information regarding incidents to VITA/Customer and do not provide information about the incidents to outside sources.	Y	
R218.	15. Record timelines, actions, and events in accordance with VITA Rules and the Incident Management System instructions in the event of a Security Incident.	Y	
R219.	16. Provide reports in the Security Dashboard of all Security incident response details and activities.	Y	
R220.	17. Follow the escalation notification processes in accordance with VITA Rules when Supplier identifies or is made aware of a security violation.	Y	
R221.	18. Participate in and, at Customer's request, conduct annual Security Incident response management exercises and provide recommendations for improvements based on the lessons learned.	Y	
R222.	19. Develop an Information Security Incident Management Plan according to VITA requirements and the Service Management Manual (IS-IMP).	Y	
R223.	20. Invoke and execute the IS-IMP, in cooperation with Customers whenever an Incident threatens the security and safety of VITA, Customer's and Supplier's environment, or a significant sector of the Customers.	Y	
R224.	21. Document the policies that govern the response to Security Incidents.	Y	
R225.	22. Document and implement the specific processes and tools for managing and responding to Security Incidents in cooperation with VITA and Customers.	Y	
R226.	23. Provide for the tracking and recording of Security Incidents.	Y	
R227.	24. Classify an incident based on established procedure or as classified by VITA.	Y	
R228.	25. Follow the escalation notification processes in accordance with security requirements and VITA Rules upon identification of a Security Incident, or potential Security Incident.	Y	
R229.	26. Record timelines, actions, and events in accordance with VITA security requirements and VITA Rules.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R230.	27. Lead in the investigation of Security Incidents and report findings to VITA and VITA identified parties.	Y	
R231.	28. Lead in the creation of a remediation plan that is acceptable to VITA and Customers.	Y	
R232.	29. Participate with the management and execution of the VITA approved remediation plans across the environment.	Y	
R233.	30. Conduct a forensic investigation to determine what Systems, data and information have been affected by the Security Incident.	Y	
R234.	31. Facilitate the identification of the initial point of entry into the environment, or other source of the Security Incident; including the tools and methods employed by the intruders, any data compromised, as well as a list of all other systems, Applications, or Third Parties potentially compromised.	Y	
R235.	32. Coordinate investigation activities in conjunction with VITA and Customer to maintain the data integrity of any asset which may be needed for evidence.	Y	
R236.	33. Coordinate the collection of any data or hardware deemed necessary by VITA and Customers to assist with the Security Incident response, including logs, disk drives, files, servers, work stations, and other items which may be of evidentiary value.	Y	
R237.	33.1. Maintain evidence integrity and strict chain of custody procedures for any items (physical or logical) relating to the Security Incident response investigation.	Y	
R238.	33.2. Assist VITA in determining the impact and scope of suspected security incidents.	Y	
R239.	33.3. Establish a Root Cause Analysis process for determining the underlying causes of a Security Incident.	Y	
R240.	33.4. Establish a corrective action process based on RCA findings that leads to actions that avoid or mitigate future Security Incidents.	Y	
R241.	34. Train and designate the security leads within Supplier and Service Tower Providers that will have ownership and responsibility for handling Security Incidents.	Y	
R242.	35. Facilitate and provide for a Computer Security Incident Response Team (CSIRT) that with other subject matter experts is tasked to respond to Security Incidents in accordance with VITA and Customer IT security requirements, processes and required response times.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R243.	36. Conduct an annual Security Incident Management response exercise with VITA to validate the Security Incident response processes.	Y	
R244.	36.1. Report results from the Security Incident Management response exercises and provide recommendations for improvements to VITA.	Y	
R245.	37. Do not serve any notice or otherwise publicize a Security Incident without the prior written consent of VITA.	Y	
R246.	38. Cooperate with any law enforcement officials, regulatory officials, agencies or associations, where Directed by VITA and with the consent of VITA.	Y	
R247.	39. Provide reports in the Portal of all Security Incident response details and activities.	Y	
R248.	40. Provide a summary of all Security Incidents related to the Services and VITA Data to VITA, upon the request of VITA, for all Security Incidents since Commencement.	Y	
R249.	41. Maintain records of all Security Incidents related to the Services and VITA Data and provide them to VITA using a real-time function.	Y	
R250.	42. Must not close an Incident until VITA/Agency is satisfied with all aspects of the investigation and all required data is provided.	Y	
R251.	**3.1.4 Rapid Malware Response**		
R252.	*Supplier will rapidly and appropriately respond to Malware outbreaks, such as virus and phishing attacks.* *Supplier's responsibilities include:*		
R253.	1. Provide the technical expertise, leadership and oversight to manage and resolve security incidents such as Malware outbreaks.	Y	
R254.	2. Contain Malware compromises to prevent further spread.	Y	
R255.	3. Identify, clean, and prevent malicious binaries from executing within the environment.	Y	
R256.	4. Identify and provide malicious and suspicious URLs to designated personnel to categorize URLs as malicious.	Y	
R257.	5. Handle requests to scan for Malware on demand in accordance with the Service Management Manual and VITA Rules.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R258.	6. Manage phishing attempts and work with necessary teams to remediate and block related phishing attempts.	Y	
R259.	7. Provide the technical expertise, leadership and oversight to manage phishing outbreaks.	Y	
R260.	8. Provide a solution that can identify users who responded to the phishing attacks.	Y	
R261.	9. React and rate events related to systems or users with access to sensitive data (e.g. HIPAA), based on the sensitivity of the data or device.	Y	
R262.	10. Maintain the capability to reverse engineer Malware to provide a detailed analysis of attack vectors.	Y	
R263.	**3.1.5 Major Security Incident Response**		
R264.	*Supplier will deliver Major Security Incident Response, as a specialized form of Security Incident Response, to provide swift action to address potential breaches and data loss with high degree of urgency. Major Security Incidents are characterized by being pervasive, large in scope, or affecting sensitive information.* *Supplier's responsibilities include:*		
R265.	1. Develop and document the standard process for managing Security Incidents from identification through closure.	Y	
R266.	2. Document protocols for declaring Security Incidents in compliance with VITA Rules, Customer policies and state statutes.	Y	
R267.	3. Provide identification and assignment of the Incident, and the execution of the applicable processes, to a dedicated Security Incident Coordinator that provides an appropriate level of dedicated attention to the Security Incident.	Y	
R268.	4. Formulate a team, scoped as appropriate to the type of Security Incident, to work under the leadership of the Security Incident Coordinator, in order to concentrate on the Security Incident and ensure that adequate resources and focus are provided to finding a timely resolution.	Y	
R269.	5. Provide management and control of the Security Incident from identification to resolution, including the following:	Y	
R270.	5.1. Review the proposed resolution time for each Security Incident with VITA and Customer, and update the status accordingly.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R271.	5.2. Coordinate Security Incident tracking efforts, and provide and maintain regular communications between all parties until Security Incident resolution.	Y	
R272.	5.3. Keep Customer informed of changes in Security Incident status throughout the incident life cycle, in accordance with VITA Rules.	Y	
R273.	5.4. Keep Customer informed of changes in anticipated resolution times.	Y	
R274.	6. Provide regular communication to Customer on what happened, what is being done to fix, and what was affected.	Y	
R275.	7. Facilitate Customer notifications to required entities based on the type of Security Incident.	Y	
R276.	**3.1.5.1 Third Party Incident Response Retainer**		
R277.	*This section identifies requirements for Supplier to offer an on-demand third party incident response service to immediately begin assessing and responding to an information security incident. Supplier responsibilities are those detailed in Section 3.1 above.* *Supplier will offer these services in the following ways:*		
R278.	1. Annual Incident Response Retainer, in which customers pay an annual fee and receive service as needed.	Y	
R279.	2. Unused retainer fees will be creditable towards other services offered by the Supplier.	Y	
R280.	3. On-demand Response Retainer, in which customers pay no annual fee and receive and pay for services on an as-needed basis.	Y	
R281.	**3.1.5.2 Response Preparedness**		
R282.	*This section identifies requirements for Supplier to develop plans to prepare customer organizations to respond quickly and effectively to a security incident.* *The activities of Response Preparedness produce a Security Response Plan and provides verification through regularly scheduled test exercises that the Customer can respond to Security Incidents within the required and agreed upon business time frames.* *Supplier's responsibilities include:*		
R283.	1. Develop and maintain a Security Response Plan that defines the activities, and schedules for exercises, to verify the Customer can respond to a Security Incidents.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R284.	1.1. Develop test objectives and success criteria with the Customer designed to verify that Customer's IT organization, security organization, other Suppliers and designated Third Party vendors can respond to a Security Incident.	Y	
R285.	1.2. Obtain and document Customer approval of the test objectives and success criteria.	Y	
R286.	1.3. Identify all the required IT technical and services operations (including computer systems, networks, Applications, data repositories, telecommunications, environment, technical support and Service Desk) for test execution.	Y	
R287.	1.4. Coordinate with Customer, other Suppliers and designated Third Party vendors to establish a schedule and calendar of test activities.	Y	
R288.	2. Schedule testing dates in cooperation with the Customer, its designees, other Suppliers, and other Third Party vendors.	Y	
R289.	3. Test all components of the Security Response Plan in cooperation with the Customer, its designees, other Suppliers, and any other Third Party vendors.	Y	
R290.	3.1. Test execution will demonstrate, at a minimum, the validity of the Security Response Plans ability to respond to Security Incidents.	Y	
R291.	3.2. Ensure that all testing activities are conducted in such a manner so that active production, test, and development environments are not impacted.	Y	
R292.	3.3. Notify Customers of any anticipated risks, where a Customer may choose to exclude the impacted services or systems from a portion of the testing.	Y	
R293.	3.4. Evaluate the results of the test and identify potential corrective actions.	Y	
R294.	3.5. Provide initial test results to the Customer and incorporate Customer feedback into the final test results report.	Y	
R295.	4. Provide Customer with a formal report of the test results within thirty (30) days of each test; at a minimum, these reports should include:	Y	
R296.	4.1. The results achieved	Y	
R297.	4.2. A comparison of the results to the measures and goals identified in the Security Response plan	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R298.	4.3. A plan and a schedule, to remediate any Security Incident Response issues identified during testing	Y	
R299.	5. Retest within ninety (90) days if any test objectives are not met due to Supplier failure to coordinate and schedule between the Customer, its designees, other Suppliers, or other Third Party vendors.	Y	
R300.	6. Execute response preparedness plan activities at a minimum annually.	Y	
R301.	**3.1.6 Threat Analysis and Intelligence**		
R302.	*Supplier will develop plans to correlate information gathered about an environment with knowledge of threats to assist in structuring pro-active response to credible threats. Supplier's responsibilities include:*		
R303.	1. Develop a profile of threats in the environment.	Y	
R304.	1.1. Gather and correlate threat data from multiple sources including device logs, security devices, SIEM systems etc. to develop a catalog of potential threats.	Y	
R305.	1.2. Identify potential resources, tools, and techniques that could be used to exploit the identified threats.	Y	
R306.	1.3. Catalog a subset of credible threats based on potential threats, resources, tools, and techniques.	Y	
R307.	2. Gather information regarding susceptibility of the customer environment to credible threats.	Y	
R308.	2.1. Identify vulnerabilities in the customer environment from sources including vulnerability scans.	Y	
R309.	2.2. Identify the value of customer information assets to attackers.	Y	
R310.	2.3. Catalog a subset of high-priority threats based on credible threats, vulnerabilities, and value.	Y	
R311.	3. Identify recommended mitigation measures to counter high-priority threats.	Y	
R312.	4. Report the threat analysis in a format as specified in the Service Management Manual.	Y	
R313.	5. Provide an analysis of security patches impacting the environment at least weekly.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R314.	**3.1.7 Security Operations Center**		
R315.	*This section identifies requirements for providing a dedicated, United States-based site from which provider personnel manage, monitor, assess, and defend information technology assets.*		
R316.	Supplier will establish and maintain a Security Operations Center, which will monitor and report on all aspects of the Services.	Y	
R317.	**3.1.7.1 General Security Operations Center Service Requirements**		
R318.	*Supplier's responsibilities include:*		
R319.	1. The service delivery process must not compromise the confidentiality, availability, and integrity of the Commonwealth's assets, including software, hardware, and data.	Y	
R320.	2. The Supplier will not compromise the confidentiality of the state's operational security posture, vulnerability status, and attack status.	Y	
R321.	3. The Supplier's storage, transmission, display, and access of state data will remain, at all times, within the United States.	Y	
R322.	4. Shared service delivery environments must maintain sufficient technical and organizational capacity to support the needs of the state in the event of a catastrophic event that causes simultaneous severe information security incidents for many or all of its customers.	Y	
R323.	5. All communications between elements and components of the Security Operations Center infrastructure will be encrypted.	Y	
R324.	6. The service delivery model must scale to accommodate new operational locations, growth in network traffic, and increasing and changing threats.	Y	
R325.	7. All Security Operations Center components will be supported by a centralized problem reporting and resolution system staffed twenty-four hours a day, seven days a week.	Y	
R326.	8. Coordinate and collect security operation information from Suppliers.	Y	
R327.	**3.1.7.2 Security Operations Center Functional Requirements**		
R328.	*The Security Operations Center will:*		
R329.	1. Be staffed twenty-four hours a day, seven days a week, each day of the year (24x7x365).	Y	
R330.	2. Work with VITA and Customer employees, contractors, consultants, and other vendors to resolve security incidents in accordance with incident response requirements.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R331.	3. Operate twenty-four hours a day, seven days a week, each day of the year (24x7x365) to receive incoming security data from multiple sources, correlate the security data, and provide real-time alerting and reporting.	Y	
R332.	4. Provide denial of service mitigation controls and denial of service attack reporting information. This information should include network utilization and attack data.	Y	
R333.	5. Generate real time security alerts, trend analyses, and reports.	Y	
R334.	6. Map attack vectors and sites of alerts in real-time on a topological map of the state's information technology infrastructure.	Y	
R335.	7. Provide for fine-tuning of alerts and priority alert classification of types of attacks.	Y	
R336.	8. Correlate data between input streams to point out attacks which may be unnoticeable from a single point of input.	Y	
R337.	9. Receive and analyze security data from the security and devices in the environment.	Y	
R338.	10. Provide emergency notification for identified security alerts, issues, or incidents.	Y	
R339.	11. Handle all security alerts generated in the environment and is responsible for the initial triage.	Y	
R340.	12. Coordinate activities among experts in order to resolve a security event and maintain a log of actions.	Y	
R341.	**3.1.7.3 Security Operations Center Technical Requirements**		
R342.	*The Security Operations Center will:*		
R343.	1. Be based on best practices.	Y	
R344.	2. Be able to accept input from a wide range of devices including routers, IDS/IPS/HIDS, firewalls, logging system(s), applications, servers, etc.	Y	
R345.	3. Provide for secure logon and communications to SOC systems for remote management.	Y	
R346.	4. Provide a time between receipt of verified alerts and the notification of customer personnel based on severity of the alert.	Y	
R347.	5. Scale to support the Commonwealth environment inputs over secure channels.	Y	
R348.	**3.1.7.4 Security Operations Center Operational Requirements**		
R349.	*The Security Operations Center will:*		

Ref#	Requirement	Comply (Y/N)	Supplier Response
R350.	1. Monitor, escalate and record alerts and Security Events at all times - 24x7x365.	Y	
R351.	2. Classify alert and security event severity based on Customer requirements.	Y	
R352.	3. Make contact with the documented responsible party for the affected service, software, equipment, etc. with the initial assessment of the security event or alert based upon the event or alert classification.	Y	
R353.	4. Investigate alerts and events from Applications and infrastructure to proactively identify any security-related issues.	Y	
R354.	5. Continuously tune alerts and their severity, and provide recommendations to VITA about tuning the events and alerts from Tools such as intrusion detection and prevention Systems, deep packet inspection devices, etc.	Y	
R355.	6. Gather intelligence by analyzing reports, interviewing Customers, and examining logs to identify Events, risk, exposure, compliance, and suspicious activity throughout the infrastructure network(s).	Y	
R356.	7. Provide URL content analysis to identify suspicious/malicious destinations and then perform URL re-categorization and/or URL blocking as required in the infrastructure content filtering and web security solution.	Y	
R357.	8. Assess, coordinate, and recommend recovery steps.	Y	
R358.	9. Close security events, to include support case closure and, where required, root cause reporting.	Y	
R359.	10. Own, monitor, track, and communicate security event reports back to Customer (e.g., immediate report, root cause analysis report, monthly summary reports).	Y	
R360.	11. Keep designated Supplier, Customer and Customer authorized third party contacts informed on status and progress.	Y	
R361.	12. Receive and respond to escalation from any Supplier, Customer or Customer authorized third party help desk or support group for any security-related issues.	Y	
R362.	13. Receive and respond to escalation calls or contact for any security-related issues.	Y	
R363.	14. Provide a technical recovery team to assist with response and remediation of Security Incidents and large-scale Security Events.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R364.	15. Ensure compliance per the Service Management Manual of systems involved in remediation efforts.	Y	
R365.	16. Provide Customer a portal view using approved or existing tools into currently open Security Event tickets and ad hoc reporting of any and all Security Events, Security Incidents and other security cases.	Y	
R366.	17. Produce and provide Customer with real-time, daily, weekly, monthly, quarterly, and yearly reports by Customer defined demographics detailing events received and resolved as well as current trends in our security environment, including attack vectors, root cause analysis and case volumes.	Y	
R367.	18. Provide input for the Security Dashboard that includes the statistics for the previous month, current status of the security environment, as well as any changes or upgrades planned for the coming month.	Y	
R368.	**3.1.7.5 Vulnerability Scanning**		
R369.	*This section identifies requirements for scanning of particular devices and subnets for known vulnerabilities.* *Supplier's responsibilities include:*		
R370.	1. Pre-Production	Y	
R371.	1.1. Scan any applicable new Systems, devices, or ~~Application Software~~ (or any Systems ~~or Software~~ to be deployed in a new project). Scans will include an operating system scan, a web vulnerability scanning for Web servers, and any other applicable scan types identified in the Service Management Manual.	Y	(Application Scanning suspended on MOD 23 Effective Date)
R372.	1.2. Rescan the system and notify the owner of the results.	Y	
R373.	1.3. Ensure that no System or Application is moved into production until any identified vulnerability is corrected or an exception has been granted.	Y	
R374.	1.4. Conduct pre-production consulting with the teams responsible for the assets in question on an ad-hoc basis.	Y	
R375.	2. Production	Y	
R376.	2.1. Perform security vulnerability assessments in accordance with security requirements.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R377.	2.2. Document and communicate the scan results and recommend remediation activities to reduce security risks.	Y	
R378.	2.3. Coordinate and track to completion any remediation tasks related to any vulnerabilities discovered.	Y	
R379.	2.4. Perform scheduled vulnerability scans as required by policy, statute or federal program guidelines and VITA Rules.	Y	
R380.	2.5. Review scan results and identify the vulnerabilities which require remediation.	Y	
R381.	3. Application Scanning	Y	(Application Scanning suspended on MOD 23 Effective Date)
R382.	3.1. Scan Applications as requested by Customer in order to evaluate, test and recommend security maintenance activities including upgrades, patches, and fixes.	Y	(Application Scanning suspended on MOD 23 Effective Date)
R383.	3.2. Work with the Application's owner or external vendor to remediate Application scan vulnerability issues.	Y	(Application Scanning suspended on MOD 23 Effective Date)
R384.	3.3. Scan Applications on a frequency defined by the Service Management Manual.	Y	(Application Scanning suspended on MOD 23 Effective Date)
R385.	3.4. Application scans should be completed using an approved tool designed for application scanning.	Y	(Application Scanning suspended on MOD 23 Effective Date)
R386.	4. Network Scanning	Y	
R387.	4.1. Scan network devices in order to identify any deviations from specified configurations, misconfigurations, or device vulnerabilities.	Y	
R388.	4.2. Report detected vulnerabilities and non-compliance issues as defined in the Service Management Manual.	Y	
R389.	5. Vulnerability Scanning Reporting	Y	
R390.	5.1. Provide an updated vulnerability scan report once every calendar month.	Y	
R391.	5.2. Report will be available via a portal that allows filtering on required reporting areas.	Y	
R392.	5.3. Vulnerability scan report will at a minimum include the following fields. The report should be able to sort on each field.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R393.	5.3.1. The target IP address	Y	
R394.	5.3.2. The vulnerabilities discovered	Y	
R395.	5.3.3. CVSS scores and the CVE and where applicable CWE of the vulnerabilities discovered	Y	
R396.	5.3.4. Severity level of vulnerabilities discovered	Y	
R397.	5.3.5. Description of vulnerability	Y	
R398.	5.3.6. Affected software, firmware, and/or hardware	Y	
R399.	5.3.7. Indication of whether the vulnerability is confirmed by the tool or is a potential vulnerability	Y	
R400.	5.3.8. Vulnerability identifiers	Y	
R401.	5.3.9. List of the target's open ports	Y	
R402.	5.3.10. Host information such as device name, MAC address, NetBIOS name, etc.	Y	
R403.	6. Each vulnerability scan report will include corresponding recommendations for remediation.	Y	
R404.	7. Supplier will work with the owner of vulnerable system to advise, complete, and develop remediation plans and take any approved steps necessary to correct the issue.	Y	
R405.	**3.1.7.6 Penetration Testing**		
R406.	*This section identifies requirements for penetration testing. The Supplier will provide penetration testing as part of security services.* *Supplier's responsibilities include:*		
R407.	1. Have an independent third party perform at least once annually external penetration testing (from outside of the Customer Environment), using a variety of tools in accordance with industry best practices to attempt to gain access to the environment. The test should attempt to gain as much access as possible (i.e. enterprise level administrator access). Testing will include all Customer and Supplier Environments.	Y	
R408.	2. Have an independent third party perform at least once annually internal penetration testing (from within the Customer Environment), using a variety of tools in accordance with industry best practices to attempt to gain access to the environment. The test	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
	should attempt to gain as much access as possible (i.e. enterprise level administrator access). Testing will include all Customer and Supplier Environments.		
R409.	3. Provide the final results and any related work product for review within 30 days of test completion.	Y	
R410.	4. The rules of engagement for the independent third party are subject to approval prior to initiation of the penetration test.	Y	
R411.	5. Scope of the penetration test should include a material representation of the different configurations throughout the environment and/or as requirements as described in the Service Management Manual. The scope will be approved by VITA prior to implementation of the penetration test.	Y	
R412.	6. Work with the owner of vulnerable system to advise, complete, and develop remediation plans and take any approved steps necessary to correct the issue.	Y	
R413.	7. Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub- network added to the environment, or a web server added to the environment).	Y	
R414.	8. Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment.	Y	
R415.	9. Verify that noted exploitable vulnerabilities were corrected and testing repeated.	Y	
R416.	10. Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists.	Y	
R417.	11. Verify that the penetration test includes network-layer penetration tests.	Y	
R418.	12. Verify that the penetration test includes application-layer penetration tests.	Y	
R419.	13. Network Layer Testing, which includes testing of the network devices such as servers, firewalls, routers and switches to identify security weaknesses such as unpatched systems, default passwords and misconfigured devices.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R420.	14. Web Application Testing, which includes testing of the web application's authentication mechanisms, input screens, and functionality and user roles to identify security weaknesses in the development of the application. A-LIGN's web application testing identifies common vulnerabilities such as those published by OWASP and SANS Top 20, as well as those unique to the web application.	Y	(Application Scanning suspended on MOD 23 Effective Date)
R421.	15. Social Engineering, which includes a testing method used to extract information or gain physical access to a location through the end-user. This may include phones calls or emails to targeted individuals, or attempting to bypass physical controls to access sensitive information.	Y	
R422.	16. Report preparation will start with overall testing procedures, followed by an analysis of vulnerabilities and risks. The high risks and critical vulnerabilities will have priorities and then followed by the lower order. However, while documenting the final report, the following points needs to be considered:	Y	
R423.	16.1. Overall summary of penetration testing	Y	
R424.	16.2. Details of each step and the information gathered during the pen testing	Y	
R425.	16.3. Details of all the vulnerabilities and risks discovered	Y	
R426.	16.4. Details of cleaning and fixing the systems	Y	
R427.	16.5. Suggestions for future security	Y	
R428.	**3.1.7.7 Compliance Management**		
R429.	*The Supplier will provide a solution that will ensure systems and web application infrastructure resources maintain compliance with security configuration requirements of VITA Rules at all times.* *Supplier's responsibilities include:*		
R430.	1. Produce on demand and scheduled compliance reports.	Y	
R431.	2. Provide a system able to evaluate all devices within the VITA, Customer's and Supplier's environment for compliance with configuration settings.	Y	
R432.	3. Evaluate all software devices and applications within the VITA, Customer's and Supplier's environment for compliance with configuration settings.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R433.	4. Use industry regulations and standards as well as customized rule sets for evaluating whether a configuration is in compliance	Y	
R434.	5. Provide a multi-tenant portal that will provide the compliance check results to each agency. The portal will limit the results of the compliance check to the device owning agency and to VITA.	Y	
R435.	6. Integrate into the device provisioning process, verifying configurations are in compliance prior to deployment within the environment.	Y	
R436.	7. Identify any system out of compliance and should be reported for remediation to the identified parties.	Y	
R437.	8. Provide details regarding the version and patch status of software and applications installed on each device.	Y	
R438.	9. Support performing compliance checks in a distributed environment.	Y	
R439.	10. Support on demand scanning.	Y	
R440.	11. Support unmanaged and managed devices.	Y	
R441.	12. Identify unmanaged devices and perform pre-connect compliance check.	Y	
R442.	13. Assess all compliance data based on industry standard controls as mapped to Customer's security policies and external regulations. The controls will be maintained and made current at least annually.	Y	
R443.	14. Run compliance scans of servers, network devices, etc. to ensure they have not been reconfigured without authorization.	Y	
R444.	15. Scan the external facing software application or device to ensure compliance with VITA Rules.	Y	(Application Scanning suspended on MOD 23 Effective Date)
R445.	16. Work with the Customer to bring the resource back into compliance in accordance with Service Management Manual.	Y	
R446.	17. Provide compliance check scan reports monthly and on demand when requested by the Customer.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R447.	**3.2 Perimeter Network Security**		
R448.	*This section includes requirements pertaining to security controls between the internet and other external connections. These security controls are designed to protect the environment from threats originating outside of the Customer networks and Managed Environment.*		
R449.	**3.2.1 Managed IDS/IPS**		
R450.	*Supplier will offer centrally-managed services for configuration, monitoring, change management, and support of Intrusion Detection System (IDS) and Intrusion Preventions System (IDS) devices regardless of device and software ownership.* *Supplier's responsibilities include:*		
R451.	1. Provide expertise and participate in network design and change discussions.	Y	
R452.	2. Install network intrusion detection systems and network intrusion prevention systems.	Y	
R453.	3. Integrate and manage event logging into the SIEM solution in accordance with the Service Management Manual.	Y	
R454.	4. Provide IDS/IPS documentation and representation to support all external audit requests.	Y	
R455.	5. Provide designated personnel access to view and query real-time events, historical events, policies, rules, device settings for each intrusion IPS/IDS device, and any other data identified in the Service Management Manual.	Y	
R456.	6. Provide custom dashboards for focused views of IDS/IPS data for the program, each individual customer and other authorized parties, as requested.	Y	
R457.	7. Evaluate network design, Systems and Applications, and traffic patterns when defining policy and rule settings. Out-of-the-box intrusion prevention System policy and signature settings are not acceptable.	Y	
R458.	8. Provide a report for each IDS/IPS device that is deployed, documenting the justification for its policy parameters and signature tuning.	Y	
R459.	9. Provide a detailed listing of all active and inactive IDS/IPS signature and policy components upon request.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R460.	10. Provide a documented assessment of network architecture, systems, ~~Applications~~ and traffic patterns for each deployed IDS/IPS device and findings as they relate to policy and signature settings. The report will include recommendations and next steps for adjusting policy and signature components. This report will be presented as identified in the Service Management Manual.	Y	(Application Scanning suspended on MOD 23 Effective Date)
R461.	11. Document a technical assessment of IDS/IPS capacity management for each IDS/IPS device, including historical data and future projections of individual IDS/IPS device metrics as defined in the Service Management Manual.	Y	
R462.	12. Coordinate a meeting with individuals designated to review all aspects of IDS/IPS architecture, policy components and signatures for each monitored network. This will include:	Y	
R463.	12.1. The report on IDS/IPS policies and signatures described below	Y	
R464.	12.2. A discussion of new threats and attack trends	Y	
R465.	12.3. A summary of alerts processed over the previous quarter	Y	
R466.	12.4. Proactive discoveries made by the Supplier	Y	
R467.	13. Respond to requests to research any IDS/IPS signatures related to Customer-perceived threats. This may result from a new patch or internal investigation.	Y	
R468.	14. Define a process to review vulnerability announcements from all vendors and security organizations identified in the Service Management Manual. Incorporate applicable IDS/IPS rules (current and future) into IDS/IPS policies.	Y	
R469.	15. Provide properly experienced and trained network security analysts to participate with the SOC in review of IDS/IPS alerts in real-time.	Y	
R470.	16. Incorporate the Service Management Manual defined threat matrix scoring system into the alert review and escalation process.	Y	
R471.	17. Provide an alert communication template to be used with notifications and escalations. The template will include:	Y	
R472.	17.1. An event summary	Y	
R473.	17.2. Summary of the threat matrix rating	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R474.	17.3. An analyst brief on the signature fired, the source, target systems, vector and attack type as it relates to Customer exposure	Y	
R475.	17.4. An analyst brief of false positive analysis	Y	
R476.	17.5. An analyst brief of packet capture analysis	Y	
R477.	18. Implement ad hoc requests to change signature and policy settings in accordance with the Service Management Manual.	Y	
R478.	19. Provide expertise to create and deploy IDS/IPS signatures.	y	
R479.	20. Provide full, un-obfuscated rule syntax for vendor-provided IDS/IPS rules as requested. This will be used to evaluate rule effectiveness, escalated alerts and false positives.	Y	
R480.	21. Provide full packet captures for alerts upon request within format specified by Service Management Manual.	Y	
R481.	22. Coordinate and develop an alert escalation process with VITA, Customer, authorized third-party contacts, and any other parties identified in the Service Management Manual.	Y	
R482.	23. Provide IDS/IPS devices with the capability to disable inline blocking for individual devices and/or individual signatures.	Y	
R483.	24. Provide an inline testing environment replicating key ingress/egress traffic to test and validate signatures. This traffic will simulate or mirror production traffic.	Y	
R484.	25. Upgrade the network IPD/IPS devices and all associated rules, signatures, settings and software when upgrades are provided by the applicable vendor, when such upgrades are in accordance with industry best practices, or as required to maintain compliance with security requirements.	Y	
R485.	26. Update, configure and maintain network intrusion detection and prevention Systems.	Y	
R486.	27. Create a risk exception for Customer approval for any network device that cannot be configured, maintained or updated.	Y	
R487.	28. Bypass inline IDS/IPS devices. Workflows will exist for both logical (Software) bypass and physical (cabling) bypass of inline traffic processing. Bypasses will exist as emergency procedures in the event of perceived impact from IDS/IPS devices.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R488.	29. Provide prerequisites and workflows for restoring bypassed inline IDS/IPS devices.	Y	
R489.	30. Install updates that address known vulnerability or risks to the network-based IDS/IPS devices as such updates are identified by the vendor of the network-based IDS/IPS, and when such updates are made available.	Y	
R490.	31. Configure updates to the network-based intrusion prevention Systems as needed, directed by VITA, or specified in the Service Management Manual.	Y	
R491.	32. Configure the network-based IDS/IPS to comply with security requirements, in order to identify suspicious patterns that may indicate abnormal activity or intrusion attempts and to block events as applicable.	Y	
R492.	33. Perform ongoing tuning of the network IDS/IPS, systems signatures and configuration settings to minimize invalid alerts, i.e., false positives, false negatives, incorrectly blocked traffic, nuisance alerts, etc. Such tuning will be authorized and documented.	Y	
R493.	34. Configure the network IDS/IPS to identify Security Events that may indicate abnormal activity or intrusion attempts and block these events as applicable in accordance with the Service Management Manual.	Y	
R494.	35. Evaluate technology improvements for network IDS/IPS; provide information regarding such technology improvements, and provide recommendations on a quarterly basis.	Y	
R495.	36. Provide real-time monitoring and prevention of known and unknown attacks as well as monitoring for abnormalities that could indicate an attack.	Y	
R496.	37. IDS and IPS devices must be able to establish a baseline of normal user pattern and anything that deviates from the baseline should be flagged as a possible attack.	Y	
R497.	**3.2.2 Web Content Filtering**		
R498.	*This section identifies requirements for centrally-managed web content filtering in the environment to prevent access to inappropriate web sites regardless of device ownership, including updates and support both for base software, signatures, and site reputation. Supplier's responsibilities include:*		
R499.	1. Provide and manage a solution to filter and protect HTTP and HTTPS at a minimum, regardless of the actual TCP ports used by the traffic, and regardless of how the traffic is initiated from the device (e.g. browser, other software installed on machine).	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R500.	2. Limiting incremental latency (including incremental network latency) for Internet content to 60 milliseconds or as defined in the Service Management Manual.	Y	
R501.	3. Content Filtering Policy.	Y	
R502.	4. Provide ability to support filtering policies for multi-tenant environment; content filtering policies should be defined by assigning dispositions to Web site categories.	Y	
R503.	5. Provide these options for each category:	Y	
R504.	5.1. Allow	Y	
R505.	5.2. Block	Y	
R506.	5.3. Continue: User presented with a message containing a click-through link; user will click the link in order to access the site	Y	
R507.	5.4. Quota: User permitted to access sites in specified category for a defined period of time and/or bandwidth consumption per day	Y	
R508.	6. If a given URL is associated with multiple categories, the most restrictive option will win.	Y	
R509.	7. Provide ability to override default categorization: all users, one or more groups of users, and individual users.	Y	
R510.	8. Provide ability to assign content filtering policies at the user level (machine or Customer location level).	Y	
R511.	9. Provide ability for the content filtering policy assigned to an on-network user to follow the user from one Customer location to another Customer location.	Y	
R512.	10. Provide ability for roaming users (those not connected to Customer network) to have a content filtering policy that may be different (e.g., more liberal) than when the same user is connected to the Customer network.	Y	
R513.	11. Provide the ability to apply content filtering policies per IP address.	Y	
R514.	12. Provide ability to create custom block, continue, and quota pages.	Y	
R515.	13. Provide ability to use a custom block, continue, or quota page on a per-category basis.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R516.	14. Provide a multi-tenant solution with the ability to monitor browsing activity and provide reports. The activity reports should include an estimated browsing time, the number of requests for a site, the sites a user visited, and an overall dashboard showing summary information about this data for the program and each Customer.	Y	
R517.	15. User Authentication.	Y	
R518.	15.1. Provide ability to transparently authenticate users.	Y	
R519.	15.2. Authentication will be based upon existing authentication methods.	Y	
R520.	15.3. Allow for the option to require users to enter credentials in order to access Internet.	Y	
R521.	16. Content Filtering Bypass.	Y	
R522.	16.1. Provide ability for approved DNS subdomains to bypass the content filtering solution.	Y	
R523.	16.2. Provide ability to temporarily bypass the content filtering solution for an individual user when troubleshooting to confirm whether content filtering solution is the cause of an identified issue such as an Internet performance issue, or issue with an individual web site's functionality.	Y	
R524.	17. URL Categorization/Content Scanning.	Y	
R525.	17.1. Provide ability to perform dynamic (real-time) categorization via content analysis of URLs that are uncategorized or pose an elevated security risk (e.g., Web 2.0 sites; URLs with low domain age; low reputation score based on geographic location, IP reputation, or BGP AS reputation etc.)	Y	
R526.	17.2. Provide mechanism to request URL (re)categorization; mechanism will provide requestor with emailed response explaining action(s) taken on request and implementation timeframe as required in the Service Management Manual.	Y	
R527.	17.3. Provide ability to manually override URL categorization:	Y	
R528.	17.3.1. For all users on all content filtering policies	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R529.	17.3.2. For all users on a single content filtering policy	Y	
R530.	17.3.3. For a subset of users within a single content filtering policy	Y	
R531.	17.3.4. There cannot be a limit on the number of URLs that can have their default categorization overridden	Y	
R532.	17.4. Provide protection against both known and zero-day threats (including polymorphic malicious code, Malware attack and root-kits, anti-emulation functions, malicious Java/PDF files and other rich Internet Application exploits) through real-time active code analysis on both inbound and outbound content; security scanning mechanisms cannot rely exclusively on signature-based techniques.	Y	
R533.	17.5. Provide ability to selectively enable scanning of files based on file type (e.g., image files, executable files, rich internet Application files, text files, archive files, documents and office-related files, multimedia files, unknown file types, as well as custom file extensions). Selected product will be able to determine true file type of scanned files (e.g., determine if scanned file's extension type has been disguised – e.g., .exe renamed as .txt).	Y	
R534.	17.6. Provide ability to selectively enable blocking of file download based on file type (e.g., image files, executable files, rich internet Application files, text files, archive files, documents and office-related files, multimedia files, unknown file types, as well as custom file extensions), file size, URL category/categories or combination thereof.	Y	
R535.	17.7. Provide SSL/TLS decryption, inspection and re-encryption capability and ability to specify DNS domains and URL categories that will not be subjected to decryption.	Y	
R536.	18. Centralized policy management	Y	
R537.	18.1. Provide secure web-based portal(s) to manage and examine content filtering policy, run reports, look up URL categorizations, and submit URL re-categorization requests.	Y	
R538.	18.2. Provide following access roles in portal(s) providing content filtering policy management and reporting functionality:	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R539.	18.2.1. Read-only access to one or more policies.	Y	
R540.	18.2.2. Read-write access to one or more policies.	Y	
R541.	18.2.3. Access to management portal audit trail.	Y	
R542.	18.2.4. Access to reporting for one or more policies/user group(s).	Y	
R543.	19. Logging/Log Retention.	Y	
R544.	19.1. Audit trail will be maintained for all logins (both successful and unsuccessful); additions, modifications, and deletions; and reports run in the portal(s) providing content filtering policy management and reporting functionality. For logins, the public IP address from which access was attempted will be logged, in addition to the user name. For additions, modifications, and deletions, both the user making the change and the specific changes made will be logged. For reports, the user running the report as well as the report run (including applied filters) will be logged. Audit logs will be maintained for a minimum of 12 months.	Y	
R545.	19.2. Provide detailed logging of each user's Internet activity down to the individual object level. Detailed logs will include the following information: timestamp (UTC) – to at least a hundredth of a second, policy, username, machine name, machine LAN IP address, public IP address, category/categories, content type (examples: Application/JavaScript, Application/pdf, image/gif, image/jpeg, image/png, text/css, text/html, text/JavaScript, video, etc.), disposition (e.g., allowed, blocked), URI, request size, response size.	Y	
R546.	19.3. Retain detailed logs for 90 days.	Y	
R547.	19.4. Provide summary level information, which outlines activity at the (sub)domain level (excluding user/machine information), and retain such information for one year.	Y	
R548.	19.5. All logs will be sent to the SIEM in accordance with the Service Management Manual.	Y	
R549.	20. Reporting.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R550.	20.1. Provide for complete reports to be exportable in CSV, PDF, XML and any other format identified in the Service Management Manual.	Y	
R551.	20.2. Allow all types of report content to be saved (with selected report filters).	Y	
R552.	20.3. Enable all reports to be run on a scheduled basis and the result emailed to one or more email addresses and also delivered as identified in the Service Management Manual. Scheduling options will include: now (on-demand), one-time at specified date and time in the future or on a recurring basis at specified time interval.	Y	
R553.	20.4. There will not be a limitation on the number of scheduled reports.	Y	
R554.	20.5. Reports showing trends and baselines will be available.	Y	
R555.	20.6. Provide multi-tenant and program-wide detailed and summary reporting of each user's Internet activity. Detailed level reports will include the following information: Timestamp (UTC) – down to a second, Policy, Username, Machine Name, Machine LAN IP Address, Destination IP, Category/Categories, Content Type, Disposition, URI, Request Size, Response Size.	Y	
R556.	20.7. At a minimum, the following summary level reports will be available with the ability to drill down to supporting details:	Y	
R557.	20.7.1. Daily level of internet activity per user and IP.	Y	
R558.	20.7.2. Activity by category.	Y	
R559.	20.7.3. Trend information for all summary level reports.	Y	
R560.	20.8. Provide reporting on Internet activity response time: Timestamp (UTC) – down to second, Policy, Username, Site, Number of Requests, Total Request Size, Total Response Size, User Proxy Round Trip Time (seconds/request), Proxy Internet Origin Round Trip Time (seconds/request), Total Response Time (seconds/request).	Y	
R561.	20.9. All reports will support filtering by time period, username, user group(s), policy/policies, site(s), category/categories, disposition, IP address(es).	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R562.	20.10. Provide reporting on scanned and blocked file types.	Y	
R563.	20.11. Provide summary and detail level reporting on security threats blocked, by service and threat type.	Y	
R564.	20.12. Provide summary and detail level reporting on number of unique users/unique machines with activity. Also, need to be able to show trending as follows: Number of Unique Users/Unique Machines, Usernames/Machine name, Number of Requests, Total Request Size, Total Response Size, IP addresses, On-network or Off-network Location.	Y	
R565.	20.13. Report will support filtering by time period, time increment (e.g., x minutes, x hours, x days, x weeks), policy, IP address(es), total request size volume /total response size thresholds.	Y	
R566.	21. Test Environment/Phased Feature Deployment	Y	
R567.	21.1. Provide ability to test new code and features prior to production deployment.	Y	
R568.	21.2. Provide ability to phase in introduction of new features across user base.	Y	
R569.	22.Provide the capability for customers to manage their own users.	Y	
R570.	**3.2.3 Malware protection**		
R571.	*This section identifies requirements for managing Malware protection services and systems in the environment regardless of ownership.* *Supplier will use an approved Malware management security Tool to identify and protect all Supplier's Systems, data, devices and networks from Malware.* *Supplier's responsibilities include:*		
R572.	1. Install, update, upgrade, patch, operate and maintain Malware Protection Software and systems in accordance with security requirements for all Software and Equipment in the environment, including all supported operating systems and platforms.	Y	
R573.	2. Update anti-virus components on all devices within 24 hours of release and testing or in accordance with Service Management Manual and work with appropriate third-party vendors to immediately resolve issues.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R574.	3. Verify that all anti-virus components are performing within documented performance characteristics, and assist in all performance troubleshooting and testing activities.	Y	
R575.	4. Understand Customer operating systems and Applications to effectively troubleshoot performance issues related to security products.	Y	
R576.	5. Perform real-time Malware protection scanning in accordance with security requirements and the Service Management Manual.	Y	
R577.	6. Perform full analysis of all network traffic traversing the provided services. Monitor the status of the analysis, report findings, and remediate where necessary to avoid any performance or threat impact to the environment.	Y	
R578.	7. Report immediately, as defined by the Service Management Manual upon detection of suspicious activity.	Y	
R579.	8. In the case malicious activity is detected, analyze to determine the following:	Y	
R580.	8.1. Function of malicious activity	Y	
R581.	8.2. Infection vector	Y	
R582.	9. Develop methods using approved Tools, and/or work with appropriate approved vendors to provide enhanced detection and prevention processes.	Y	
R583.	10. Determine what if any data was/is compromised due to the security event. Include identified information in the security incident report.	Y	
R584.	11. Submit new Malware (zero-day) binaries to the anti-virus vendor for inclusion in the next pattern release.	Y	
R585.	12. Submit malicious URLs to Web security vendor to be classified as malicious.	Y	
R586.	13. Provide real-time Malware and malicious activity monitoring at Internet access points, using Tools to pull binaries from the live Internet stream. Actions performed on binaries include reverse engineering and exploding Malware in supported operating systems and/or as defined in the Service Management Manual.	Y	
R587.	14. Monitor DNS traffic for DNS requests to known malicious Internet addresses, interrogate URL and check for Malware, phishing, and any other malicious activity.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R588.	15. Provide the ability to re-route traffic back to a central location and run the traffic through the real-time Malware monitoring Tools.	Y	
R589.	16. Assess the scope of damage related to all Malware events.	Y	
R590.	17. Arrest the spread and progressive damage from the Malware.	Y	
R591.	18. Eradicate Malware through techniques such as reverse engineering, custom scripting in endpoint management system, and working with the anti-virus vendor.	Y	
R592.	19. Document troubleshooting steps that can be used by field associates to respond to Malware outbreaks or product issues.	Y	
R593.	20. Provide or use advanced Tools, including disassemblers, debuggers, tcpdump, and others as required.	Y	
R594.	21. Scan for Malware upon demand using vendor-supplied scan methods and custom scan methods.	Y	
R595.	22. Respond to and support the Security Incident response processes.	Y	
R596.	23. Provide proactive alerts for consumption by Users regarding current threats in the Environment or based on industry information.	Y	
R597.	24. Provide daily, weekly, monthly and quarterly reports in the Security Dashboard on Malware infections and remediation.	Y	
R598.	25. Develop custom interface services using standard APIs including those identified in the Service Management Manual, between approved anti-virus products and compliance, reporting and deployment Applications.	Y	
R599.	26. Develop interfaces using standard APIs including those identified in the Service Management Manual to provide a standard interface for other Tools to gather Malware detection data in an automated fashion.	Y	
R600.	27. Monitor anti-virus logs to detect any Malware infections.	Y	
R601.	28. Monitor logs from Web filtering, firewall, anti-virus and proactive Malware Tools for Malware infections and possible zero-day infections.	Y	
R602.	29. Integrate event logging into the SIEM solution in accordance with the Service Management Manual.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R603.	30. Develop standard and custom reports to assist in Incident inquiry, correlation and response activities.	Y	
R604.	31. Perform correlation activities to identify ongoing threats based on data and reports from VITA, Customer, Supplier, authorized third parties and industry sources.	Y	
R605.	32. Develop installation instructions for the anti-virus solution.	Y	
R606.	33. Author knowledge base articles, integrating into Systems used by the End User Support and systems support personnel.	Y	
R607.	34. Maintain license and support compliance for the anti-virus product.	Y	
R608.	35. Maintain approved anti-virus exclusions ensuring proper alignment with vendor recommendations, technology best practices, and consultation with appropriate subject matter experts.	Y	
R609.	36. Maintain an auditable approval process for anti-virus exclusions ensuring proper alignment with all applicable security policies.	Y	
R610.	37. Audit and report on anti-virus exclusions quarterly, including contacting the exclusion requester to validate that the need for the exclusion still exists.	Y	
R611.	38. Include in the quarterly report the number of exclusions, number of new exclusions, number of exclusions removed and business justification for all exclusions.	Y	
R612.	39. Rapidly deploy anti-virus component updates during critical Security Events, as directed by applicable security teams and policies.	Y	
R613.	40. Document troubleshooting steps for use by field associates in response to product issues.	Y	
R614.	41. Provide data and ad-hoc reporting to assist with forensics.	Y	
R615.	42. Develop custom scripts to assist in Malware remediation and detection.	Y	
R616.	43. Develop a process to address Malware protection requirements that are not provided by deployed anti-virus products in the Environment.	Y	
R617.	44. Provide the ability to discover and eradicate suspicious files across the VITA, Customer and Supplier environment based on hashes, file names, registry entries, paths, etc.	Y	
R618.	45. Provide the ability to blacklist or whitelist files based on names and/or hashes.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R619.	46. Provide standard and ad hoc reports from the solution that can be used for remediation, cleansing and correlation.	Y	
R620.	47. Provide analysis and recommendations from data, advising on corrective course of action.	Y	
R621.	48. Provide pro-active alerts to indicate potential Malware activity based on definable triggers and rule sets.	Y	
R622.	49. Proactively compare data from system to Malware sites for hash verification of known Malware.	Y	
R623.	50. Provide web portal allowing remote execution of multiple anti-virus engines on assets and deliver scan results back to the centralized data repository.	Y	
R624.	51. Provide dedicated Malware technology to detect and alert for Malware attacks at the network perimeter.	Y	
R625.	52. Provide a solution that can analyze encrypted traffic and a mechanism for VITA to access and utilize the said solution in accordance with the Service Management Manual.	Y	
R626.	**3.2.4 Network Forensics/Full Packet Capture**		
R627.	*This section identifies requirements for a full packet capture solution.* *Supplier's responsibilities include:*		
R628.	1. Ensure that data is coming in at line speed and that there will be no delays with the system performance.	Y	
R629.	2. Verify that the system is able to process the amount of data provided, with ability to expand.	Y	
R630.	3. Provide a full packet capture solution with enough resources to capture and record data and can display collected data quickly.	Y	
R631.	4. Provide a full packet capture solution that can easily be viewed by protocol, MAC, VLAN, geo-IP, and so on, and that data can be filtered.	Y	
R632.	5. Provide a full packet capture solution that has the ability to perform network behavior analysis (NBA) and block traffic that doesn't meet a certain policy.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R633.	6. Full packet capture solution provided by Supplier will download sample packets for inspection using a protocol analyzer if needed, or if it will send them over to the authorities in accordance with the Service Management Manual.	Y	
R634.	7. Full packet capture solution will retain and preserve the original timestamps. Timestamps will be synchronized to a common time zone.	Y	
R635.	8. Ensure that full packet capture solution will not cause a single point of failure.	Y	
R636.	9. Ensure that logs are saved and preserved.	Y	
R637.	10. Ensure the security of the packet capture solution.	Y	
R638.	11. Be aware of privacy concerns regarding full-packet capture. Supplier will be familiar with and review the relevant privacy laws that apply.	Y	
R639.	12. Decrypt captured traffic when approved by VITA and as specified in the Service Management Manual.	Y	
R640.	**3.2.5 Data Loss Prevention (DLP)**		
R641.	*Supplier will monitor data moving across Customer's network and create an audit trail of policy-violation incidents. Supplier will monitor customer 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. Supplier's responsibilities include:*		
R642.	1. Provide a highly scalable solution capable of automatically detecting or blocking transmissions containing sensitive data, encrypting emails containing sensitive data, or quarantining messages that may need approval to exit Customer's network.	Y	
R643.	2. Provide a solution that integrates with a centralized Data Loss Prevention environment.	Y	
R644.	3. Provide a solution that is not limited to individual packets. The solution will decrypt captured information and intelligently assemble traffic streams into Application-layer sessions.	Y	
R645.	4. Provide a solution that is able to understand, reassemble and review various protocols such as SMTP, HTTP, HTTPS, Instant Message, FTP, Telnet, P2P communications and applications. Network DLP will support the reassembly and investigation of Microsoft Word, Microsoft Excel, and Adobe PDF attachments.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R646.	5. Provide a solution able to add additional scanning categories and content filters (e.g., adult content, credit card information, backdoors, key logger, P2P, personal information, Social Security numbers, violent acts).	Y	
R647.	6. Provide a solution able to define shared variables to be used by rules. This may include network address ranges, strings for pattern matching, etc.	Y	
R648.	7. Provide solution able to create custom signatures using pattern matching in conjunction with other defined rule parameters as specified in the Service Management Manual.	Y	
R649.	8. Evaluate network architecture, traffic patterns, protected system types and Customer DLP requirements to define custom rules and monitoring.	Y	
R650.	8.1. Using “out-of-the-box” policy and signature settings are not acceptable.	Y	
R651.	9. Coordinate with Customer and service providers to evaluate changes to network architecture, traffic patterns, protected system types and updated Customer security requirements at a minimum annually.	Y	
R652.	9.1. Provide a report to Customer summarizing the discussion and next steps.	Y	
R653.	10. Provide senior technical contacts to evaluate and implement Customer custom rule requests.	Y	
R654.	11. Respond to requests to provide detailed listings of all rules and logic.	Y	
R655.	12. Respond to requests to research and identify rule capabilities related to Customer perceived threats (e.g. new patch, internal investigation).	Y	
R656.	13. Conduct, in accordance with Customer’s security policies, annual security scans of attached data storage at Customer facilities to look for sensitive data.	Y	
R657.	14. Provide the capability for data to be scanned at Customer facilities.	Y	
R658.	15. Provide the capability to scan for sensitive data upon demand for any device located on Customer’s network.	Y	
R659.	16. Provide the ability to scan UNIX, Linux and Windows computers, file shares, servers, databases, repositories such as SharePoint and any other systems identified in the Service Management Manual.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R660.	17. Provide the capability to add additional domestic and international regulatory classifications to scanning criteria.	Y	
R661.	18. Provide the ability to throttle the host's CPU utilization during scanning, such that scanning is non-impacting to production systems and Applications.	Y	
R662.	19. Conduct scans as Directed by VITA and/or Customer (e.g. during non-business hours).	Y	
R663.	20. Provide continuous monitoring of scan progress to ensure that it is successfully completed.	Y	
R664.	21. Provide the ability to export scan results.	Y	
R665.	22. Provide analysis of exported scan results.	Y	
R666.	23. Communicate the scan results and remediation options with VITA and/or the data owning agency.	Y	
R667.	24. Provide "per scan" metrics on file deletion, file redaction, and file encryption and false positives.	Y	
R668.	25. Provide online analysis and reporting of the remediation efforts to include "per scan" metrics on file deletion, file redaction, and file encryption and false positives.	Y	
R669.	26. Provide Customer with the trends and progress reports as listed below:	Y	
R670.	26.1. Monthly, quarterly and yearly metrics of all scans conducted to include scan dates, name of server or shares, total number of Incidents, number of file deletions, number of file redactions, number of file encryptions, number of false positives across all content policies, and any other metrics specified in the Service Management Manual.	Y	
R671.	27. Provide method for requesting scan reports upon demand.	Y	
R672.	28. Manage the validation scanning and Application configuration to remove false positives.	Y	
R673.	29. Integrate event logging into the SIEM solution in accordance with the Service Management Manual.	Y	
R674.	**3.2.6 Compliance Management**		
R675.	Supplier will participate in the compliance management program established for the environment. This participation may require deployment, implementation, and configuration of	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
	Supplier services in order to provide support for the compliance management program. The Supplier may be required to take steps such as deploy software, modify configuration, integrate with a tool, etc. to support the compliance management program.		
R676.	**3.2.7 Vulnerability Management**		
R677.	Supplier will participate in the vulnerability management program established for the environment. This participation may require deployment, implementation, and configuration of Supplier services in order to provide support for the vulnerability management program. The Supplier may be required to take steps such as deploy software, modify configuration, integrate with a tool, etc. to support the vulnerability management program.	Y	
R678.	**3.2.8 Penetration Testing**		
R679.	Supplier will participate in the penetration testing program established for the environment. The penetration testing program will require participation where identified and following procedures and requirements included in the Service Management Manual. All Suppliers will be expected to make services associated with this program available to be within the scope of the penetration testing program.	Y	
R680.	**3.2.9 Managed Firewall**		
R681.	*Supplier is responsible for all Enterprise (e.g., perimeter, core) and Non-Enterprise (e.g., departmental, local office) Firewalls. These sections have some duplicated requirements for clarity. Supplier will offer services for configuration, monitoring, change management, and support of firewall systems at designated facilities regardless of system and software ownership. Supplier's responsibilities include:*		
R682.	1. Provide and configure a secure multi-layer high availability firewall infrastructure with no single point of failure to support the Supplier and Program environment.	Y	
R683.	2. Utilize a minimum of two firewall manufacturers, approved by VITA, on separate layers to reduce exposure to any single manufacturer's exploit.	Y	
R684.	3. Ensure Firewalls have no negative impact on Network performance.	Y	
R685.	4. Integrate with the Change Management process approved by VITA and VITA Customers for the updating of firewall rules and objects, and obtain proper approvals prior to any revision.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R686.	5. Manage and update the firewall rules and objects as required.	Y	
R687.	6. Provide capability and process to expedite firewall rule change requests.	Y	
R688.	7. Respond to incidents and problems with Firewall Services.	Y	
R689.	8. Continuously monitor firewalls, and report any alerts or events to VITA and VITA Customers immediately, in accordance with the Service Management Manual, Customer's escalation and reporting procedures.	Y	
R690.	9. Provide program wide and individual Customer firewall rule set reports and configuration information via real time reporting and immediately upon request.	Y	
R691.	10. Provide support for URL and IP based firewall rules.	Y	
R692.	11. Integrate firewall services with Internet Proxy services (e.g., integration with Content Delivery Networks (e.g., Akamai)).	Y	
R693.	12. Integrate with MSI to provision Firewall Service Requests through online tools	Y	
R694.	13. Install, update, upgrade, patch, operate and maintain firewall protection Software and Systems in accordance with VITA and VITA Customer security requirements for all Software and Equipment in the environment.	Y	
R695.	14. Understand, maintain, and engineer the architecture of the solution to integrate into the identified environment.	Y	
R696.	15. Include recommendations for a firewall security profile.	Y	
R697.	16. Create and engineer security profiles and baselines for firewall appliances.	Y	
R698.	17. Administer, configure, customize and test "out-of-the-box" firewall rules that have been identified applicable for a firewall security implementation.	Y	
R699.	18. Build firewall rules that will not disrupt business, while providing a secure platform.	Y	
R700.	19. Develop firewall rules which are used to identify and where specified block Malware or insecure Applications within Customer's network. The required data for the rule may be derived from reverse engineering of Malware as well as industry security information	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
	and other threat intelligence data. Engineer firewall rules that can be used to alert on malicious traffic from within the infrastructure.		
R701.	20. Configure firewall rules so to fit into business Application models while protecting against emerging threats.	Y	
R702.	21. Create firewall rule(s) as required by security threats, vulnerabilities, and industry best practices.	Y	
R703.	22. Install and test rule updates that address known vulnerabilities or risks to endpoint systems.	Y	
R704.	23. Ensure that the firewall rules created will not interfere with the function and operations of the environment as specified within the Service Management Manual.	Y	
R705.	24. Work with customers, following established change control policies, to test and validate firewall rules.	Y	
R706.	25. Install configuration updates to the systems as needed or directed, in accordance with the following:	Y	
R707.	25.1. All changes must be tested on a test, development or appropriate systems prior to implementation.	Y	
R708.	25.2. Supplier must have intimate knowledge of Customer deployed assets and Applications to minimize possible risk to enterprise Applications.	Y	
R709.	26. Audit firewall rules that have been created in response to security threats and business continuity at least quarterly, for their technical relevance and integrity.	Y	
R710.	27. Ensure that firewall components are performing within defined performance guidelines and assist in all performance troubleshooting and testing activities.	Y	
R711.	28. Provide access to reports that will reflect on demand, daily, weekly, and monthly status of overall firewall operational and rule data.	Y	
R712.	29. Support exception handling processes and provide improvement recommendations to Customer or the Third Party Provider responsible for handling exception requests.	Y	
R713.	30. Maintain an auditable approval process for firewall rules ensuring proper alignment with all VITA and VITA Customer security policies and as established in the Service Management Manual.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R714.	31. Maintain firewall rules ensuring proper alignment with recommendations, technology best practices, and consultation with subject matter experts.	Y	
R715.	32. Perform ongoing tuning of firewall system rules, security profiles, and configuration to minimize false positives and false negatives.	Y	
R716.	33. Review the firewall events (alarms) to identify false positives and systems that need remediation.	Y	
R717.	34. Provide a method to submit firewall change requests.	Y	
R718.	35. Review new firewall change requests at least daily and as specified in the Service Management Manual.	Y	
R719.	36. Integrate logging into the SIEM solution in accordance with the Service Management Manual.	Y	
R720.	37. Design and engineer a process or infrastructure that will allow the ability to audit and review all firewall rules based on the firewall request/exception process, and determine if the firewall rules are still valid, can be deleted, or need to be updated.	Y	
R721.	37.1. Provide a portal and integration into a portal to allow VITA and Customers to review, approve, or identify for deletion firewall rules impacting the customer and/or the enterprise.	Y	
R722.	38. Generate an electronic copy of the firewall rules implemented and make a copy available to Customer in accordance with the SMM	Y	
R723.	39. The Supplier shall allow for penetration testing and vulnerability scans to be performed against the Solution.	Y	
R724.	40. The Supplier shall ensure that the Operating System and other Patches should be applied in line with the SMM and VITA Rules.	Y	
R725.	**3.2.9.1 Enclave**		
R726.	*Supplier's responsibilities include:*		
R727.	1. Provide network security services utilizing a defense-in-depth approach through enclaves (zoning) of the Enterprise network with multi-layered internal protections.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R728.	2. Manage internal firewalls at the network level to enforce a security policy between tenants, and sub-tenants.	Y	
R729.	3. Where identified manage firewalls to protect at the host level.	Y	
R730.	4.		
R731.	**3.3 Internal Network Security**		
R732.	**3.3.1 Managed IDS/IPS**		
R733.	*This section includes the security requirements for protecting the internal network which includes communication between devices within the Customer networks and the Managed Environment. Supplier will offer centrally managed services for configuration, monitoring, change management, and support of Intrusion Detection System (IDS) and Intrusion Preventions System (IDS) devices regardless of device and software ownership. Supplier will integrate with other Supplier's supporting the environment.* *Supplier's responsibilities include:*		
R734.	1. Provide expertise to participate in network design and change discussions.	Y	
R735.	2. Integrate and manage event logging in to the SIEM infrastructure in accordance with the Service Management Manual.	Y	
R736.	3. Provide intrusion prevention documentation and representation to support all external audit requests.	Y	
R737.	4. Provide designated personnel full read access to view and query real-time events, historical events, policies, rules, device settings for each intrusion prevention System device, and any other data identified in the Service Management Manual.	Y	
R738.	5. Provide custom dashboards for focused views of intrusion prevention System data for the program environment and each individual Customer, as requested.	Y	
R739.	6. Evaluate network design, Systems and Applications, and traffic patterns when defining policy and rule settings. Out-of-the-box intrusion prevention System policy and signature settings are not acceptable.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R740.	7. Provide a report for each intrusion prevention system device that is deployed, documenting the justification for its intrusion prevention system policy parameters and signature tuning.	Y	
R741.	8. Provide a detailed listing of all intrusion prevention System signature and policy components active or inactive upon request.	Y	
R742.	9. Provide a documented assessment of network architecture, Systems and Applications and traffic patterns for each deployed intrusion prevention System device and findings as they relate to policy and signature settings. The report will include recommendations and next steps for adjusting policy and signature components. This report will be presented as identified in the Service Management Manual.	Y	
R743.	10. Document a technical assessment of intrusion prevention system capacity management for each intrusion prevention system device, including historical data and future projections of individual intrusion prevention system device metrics as defined in the Service Management Manual.	Y	
R744.	11. Coordinate a meeting with individuals designated to review all aspects of intrusion prevention system architecture, policy components and signatures for each monitored network. This will include:	Y	
R745.	11.1. The report on intrusion prevention system policies and signatures described below.	Y	
R746.	11.2. A discussion of new threats and attack trends.	Y	
R747.	11.3. A summary of alerts processed over the previous quarter.	Y	
R748.	11.4. Proactive discoveries made by the Supplier.	Y	
R749.	12. Respond to requests to research and identify intrusion prevention system signatures related to Customer perceived threats. This may result from a new patch or internal investigation.	Y	
R750.	13. Define a process to review vulnerability announcements from all vendors and security organizations identified in the Service Management Manual. Incorporate applicable intrusion prevention system rules (current and future) into intrusion prevention system policies.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R751.	14. Provide properly experienced and trained network security analysts to participate with the SOC in review of intrusion prevention system alerts in real-time.	Y	
R752.	15. Incorporate the Service Management Manual defined threat matrix scoring system into the alert review and escalation process.	Y	
R753.	16. Provide an alert communication template to be used with notifications and escalations. The template will include:	Y	
R754.	16.1. An event summary	Y	
R755.	16.2. Summary of the threat matrix rating	Y	
R756.	16.3. An analyst brief on the signature fired, the source, target systems, vector and attack type as it relates to Customer exposure	Y	
R757.	16.4. An analyst brief of false positive analysis	Y	
R758.	16.5. An analyst brief of packet capture analysis	Y	
R759.	17. Implement ad hoc requests to change signature and policy settings in accordance with the Service Management Manual.	Y	
R760.	18. Provide expertise to create and deploy intrusion prevention system signatures.	Y	
R761.	19. Provide full, un-obfuscated rule syntax for vendor provided intrusion prevention system rules as requested. This will be used to evaluate rule effectiveness, escalated alerts and false positives	Y	
R762.	20. Implement vendor-recommended signatures in accordance with defined deployment standards	Y	
R763.	21. Provide full packet captures for alerts upon request as specified within the Service Management Manual.	Y	
R764.	22. Coordinate and develop an alert escalation process with VITA, Customer, all authorized third-party contacts, and any other party identified in the Service Management Manual.	Y	
R765.	23. Provide intrusion prevention system devices with the capability to disable inline blocking for individual devices and/or individual signatures.	Y	
R766.	24. Provide an inline testing environment replicating key ingress/egress traffic to test and validate signatures. This traffic will simulate or mirror production traffic.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R767.	25. Upgrade the network prevention systems and all associated rules, signatures, settings and software when upgrades are provided by the applicable vendor, when such upgrades are in accordance with industry best practices, or as required to maintain compliance with security requirements.	Y	
R768.	26. Update, configure and maintain network intrusion detection and prevention Systems.	Y	
R769.	27. Create a risk exception for Customer approval for any network device that cannot be configured, maintained or updated.	Y	
R770.	28. Install network intrusion detection systems and network intrusion prevention systems.	Y	
R771.	29. Provide capability to bypass inline intrusion prevention System devices. Workflows will exist for both logical (Software) bypass and physical (cabling) bypass of inline traffic processing. Bypasses will exist as emergency procedures in the event of perceived impact from intrusion prevention system devices.	Y	
R772.	30. Provide conditions and workflows for restoring bypassed inline intrusion prevention System devices.	Y	
R773.	31. Install updates that address known vulnerability or risks to the network-based intrusion prevention systems; as such updates are identified by the vendor of the network-based intrusion prevention systems.	Y	
R774.	32. Configure updates to the network-based intrusion prevention Systems as needed, directed by VITA, or specified in the Service Management Manual.	Y	
R775.	33. Configure the network-based intrusion prevention systems so as to comply with security requirements, in order to identify suspicious patterns that may indicate abnormal activity or intrusion attempts and to block events as applicable.	Y	
R776.	34. Perform ongoing tuning of the network intrusion prevention systems, systems signatures and configuration settings to minimize invalid alerts, i.e., false positives, false negatives, incorrectly blocked traffic, nuisance alerts, etc. Such tuning will be authorized and documented.	Y	
R777.	35. Configure the network intrusion prevention systems to identify Security Events that may indicate abnormal activity or intrusion attempts and block those events in accordance with the Service Management Manual.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R778.	36. Evaluate technology improvements for network intrusion prevention systems; provide information regarding such technology improvements, and provide recommendations on a quarterly basis.	Y	
R779.	37. Provide real time monitoring and prevention of known and unknown attacks as well as monitoring for abnormalities that could indicate an attack using heuristic and signature based methods.	Y	
R780.	38. IDS and IPS devices will be able to establish a baseline of normal user pattern and anything that deviates from the baseline should be flagged as a possible attack.	Y	
R781.	39. Provide a solution that can support Suppliers within the environment.	Y	
R782.	**3.3.2 Web Content Filtering**		
R783.	*This section identifies requirements for centrally manage web content filtering in the environment to prevent access to inappropriate web sites regardless of device ownership, including updates and support both for base software, signatures, and site reputation. Supplier's responsibilities include:*		
R784.	1. Provide ability to filter and protect HTTP and HTTPS at a minimum, regardless of the actual TCP ports used by the traffic, and regardless of how the traffic is initiated from the device (e.g. browser, other software installed on machine).	Y	
R785.	2. Limiting incremental latency (including incremental network latency) for Internet content to 60 milliseconds or as defined in the Service Management Manual.	Y	
R786.	3. Content Filtering Policy	Y	
R787.	3.1. Provide ability to support filtering polices for a multi-tenant environment; content filtering policies should be defined by assigning dispositions to Web site categories.	Y	
R788.	3.2. Provide these options for each category:	Y	
R789.	3.2.1. Allow	Y	
R790.	3.2.2. Block	Y	
R791.	3.2.3. Continue: User presented with a message containing a click-through link; user will click the link in order to access the site	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R792.	3.2.4. Quota: User permitted to access sites in specified category for a defined period of time and/or bandwidth consumption per day	Y	
R793.	3.3. If a given URL is associated with multiple categories, the most restrictive option will win.	Y	
R794.	3.4. Provide ability to override default categorization: all users, one or more groups of users, and individual users.	Y	
R795.	3.5. Provide ability to assign content filtering policies at the user level (vice machine or Customer location level).	Y	
R796.	3.6. Provide ability for the content filtering policy assigned to an on-network user to follow the user from one Customer location to another Customer location.	Y	
R797.	3.7. Provide ability for roaming users (those not connected to Customer network) to have a content filtering policy that may be different (e.g., more liberal) than when the same user is connected to the Customer network.	Y	
R798.	3.8. Provide the ability to apply content filtering policies per IP address.	Y	
R799.	3.9. Provide ability to create custom block, continue, and quota pages.	Y	
R800.	3.10. Provide ability to use a custom block, continue, or quota page on a per-category basis.	Y	
R801.	3.11. Provide a multi-tenant solution with the ability to monitor browsing activity and provide reports. The activity reports should include an estimated browsing time, the number of requests for a site, the sites a User visited, and an overall dashboard showing summary information about this data for the program and each Customer.	Y	
R802.	4. User Authentication	Y	
R803.	4.1. Provide ability to transparently authenticate users.	Y	
R804.	4.2. Authentication will be based upon existing authentication methods.	Y	
R805.	4.3. Allow for the option to require users to enter credentials in order to access Internet.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R806.	5. Content Filtering Bypass	Y	
R807.	5.1. Provide ability for approved DNS subdomains to bypass the content filtering solution.	Y	
R808.	5.2. Provide ability to temporarily bypass the content filtering solution for an individual user when troubleshooting to confirm whether content filtering solution is the cause of an identified issue such as an Internet performance issue, or issue with an individual web site's functionality.	Y	
R809.	6. URL Categorization/Content Scanning	Y	
R810.	6.1. Provide ability to perform dynamic (real-time) categorization via content analysis of URLs that are uncategorized or pose an elevated security risk (e.g., Web 2.0 sites; URLs with low domain age; low reputation score based on geographic location, IP reputation, or BGP AS reputation etc.)	Y	
R811.	6.2. Provide mechanism to request URL (re)categorization; mechanism will provide requestor with emailed response explaining action(s) taken on request and implementation timeframe as required in the Service Management Manual.	Y	
R812.	6.3. Provide ability to manually override URL categorization:	Y	
	6.3.1. For all users on all content filtering policies	Y	
	6.3.2. For all users on a single content filtering policy	Y	
	6.3.3. For a subset of users within a single content filtering policy	Y	
	6.3.4. There cannot be a limit on the number of URLs that can have their default categorization overridden	Y	
R813.	6.4. Provide protection against both known and zero-day threats (including polymorphic malicious code, Malware attack and root-kits, anti-emulation functions, malicious Java/PDF files and other rich Internet Application exploits) through real-time active code analysis on both inbound and outbound content; security scanning mechanisms cannot rely exclusively on signature-based techniques.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R814.	6.5. Provide ability to selectively enable scanning of files based on file type (e.g., image files, executable files, rich internet Application files, text files, archive files, documents and office-related files, multimedia files, unknown file types, as well as custom file extensions). Selected product will determine true file type of scanned files (e.g., determine if scanned file's extension type has been disguised – e.g., .exe renamed as .txt).	Y	
R815.	6.6. Provide ability to selectively enable blocking of file download based on file type (e.g., image files, executable files, rich internet Application files, text files, archive files, documents and office-related files, multimedia files, unknown file types, as well as custom file extensions), file size, URL category/categories or combination thereof.	Y	
R816.	6.7. Provide SSL/TLS decryption, inspection and re-encryption capability and ability to specify DNS domains and URL categories that will not be subjected to decryption.	Y	
R817.	7. Centralized policy management	Y	
R818.	7.1. Provide secure web-based portal(s) to manage and examine content filtering policy, run reports, look up URL categorizations, and submit URL re-categorization requests.	Y	
R819.	7.2. Provide following access roles in portal(s) providing content filtering policy management and reporting functionality:	Y	
R820.	7.2.1. Read-only access to one or more policies	Y	
R821.	7.2.2. Read-write access to one or more policies	Y	
R822.	7.2.3. Access to management portal audit trail	Y	
R823.	7.2.4. Access to reporting for one or more policies/user group(s)	Y	
R824.	8. Logging/Log Retention	Y	
R825.	8.1. Audit trail will be maintained for all logins (both successful and unsuccessful); additions, modifications, and deletions; and reports run in the portal(s) providing content filtering policy management and reporting functionality. For logins, the IP	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
	address from which access was attempted will be logged, in addition to the user name. For additions, modifications, and deletions, both the user making the change and the specific changes made will be logged. For reports, the user running the report as well as the report run (including applied filters) will be logged. Audit logs will be maintained for a minimum of 12 months.		
R826.	8.2. Provide detailed logging of each user's Internet activity down to the individual object level. Detailed logs will include the following information: timestamp (UTC) – to at least a hundredth of a second, policy, username, machine name, machine LAN IP address, public IP address, category/categories, content type (examples: Application/JavaScript, Application/pdf, image/gif, image/jpeg, image/png, text/css, text/html, text/JavaScript, video, etc.), disposition (e.g., allowed, blocked), URI, request size, response size.	Y	
R827.	8.3. Retain detailed logs for 90 days in a state that is easily accessible/searchable by approved customers	Y	
R828.	8.4. Provide summary level information, which outlines activity at the (sub)domain level (excluding user/machine information), and retain such information for one year.	Y	
R829.	9. Reporting		
R830.	9.1. Provide for complete reports to be exportable in CSV, PDF, XML, and any other format identified in the Service Management Manual.	Y	
R831.	9.2. Allow all types of report to be saved (with selected report filters).	Y	
R832.	9.3. Enable all reports to be run on a scheduled basis and the result emailed to one or more email addresses, and also delivered as identified in the Service Management Manual. Scheduling options will include: now (on-demand), one-time at specified date and time in the future or on a recurring basis at specified time interval.	Y	
R833.	9.4. There will not be a limitation on the number of scheduled reports.	Y	
R834.	9.5. Reports showing trends and baselines will be available.	Y	
R835.	9.6. Provide multi-tenant and program-wide detailed and summary reporting of each user's Internet activity. Detailed level reports will include the following	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
	information: Timestamp (UTC) – down to a second, Policy, Username, Machine Name, Machine LAN IP Address, Destination IP, Category/Categories, Content Type, Disposition, URI, Request Size, Response Size.		
R836.	9.6.1. At a minimum, the following summary level reports will be available with the ability to drill down to supporting details:	Y	
R837.	9.6.1.1. Daily level of internet activity per user and IP	Y	
R838.	9.6.1.2. Activity by category	Y	
R839.	9.6.1.3. Trend information for all summary level reports	Y	
R840.	9.7. Provide reporting on Internet activity response time: Timestamp (UTC) – down to second, Policy, Username, Site, Number of Requests, Total Request Size, Total Response Size, User Proxy Round Trip Time (seconds/request), Proxy Internet Origin Round Trip Time (seconds/request), Total Response Time (seconds/request).	Y	
R841.	9.8. All reports will support filtering by time period, username, user group(s), policy/policies, site(s), category/categories, disposition, IP address(es).	Y	
R842.	9.9. Provide reporting on scanned and blocked file types.	Y	
R843.	9.10. Provide summary and detail level reporting on security threats blocked, by service and threat type.	Y	
R844.	9.11. Provide summary and detail level reporting on number of unique users/unique machines with activity. Also, need to be able to show trending as follows: Number of Unique Users/Unique Machines, Usernames/Machine name, Number of Requests, Total Request Size, Total Response Size, IP addresses, On-network or Off-network Location.	Y	
R845.	9.12. Report will support filtering by time period, time increment (e.g., x minutes, x hours, x days, x weeks), policy, IP address(es), total request size volume /total response size thresholds.	Y	
R846.	10. Test Environment/Phased Feature Deployment	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R847.	10.1. Provide ability to test new code and features prior to production deployment	Y	
R848.	10.2. Provide ability to phase in introduction of new features across user base.	Y	
R849.	11. Provide the capability for customers to manage their own users.	Y	
R850.	**3.3.3 Malware protection**		
R851.	*This section identifies requirements for managing anti-virus and other Malware protection software and systems in the environment regardless of ownership.* *Supplier will use an approved Malware management security Tool to identify and protect Systems, data, devices and networks from Malware.* *Supplier's responsibilities include:*		
R852.	1. Install, update, upgrade, patch, operate and maintain Malware Protection Software and systems in accordance with security requirements for all Software and Equipment in the Environment, including all supported operating systems and platforms.	Y	
R853.	2. Update anti-virus components on all devices within 24 hours of release and testing or in accordance with Service Management Manual and work with appropriate third-party vendors to immediately resolve issues.	Y	
R854.	3. Verify that all anti-virus components are performing within documented performance characteristics, and assist in all performance troubleshooting and testing activities.	Y	
R855.	4. Understand Customer operating systems and Applications to effectively troubleshoot performance issues related to security products.	Y	
R856.	5. Perform real-time Malware protection scanning in accordance with security requirements and the Service Management Manual.	Y	
R857.	6. Upon detection of a Malware infection, respond immediately, as defined by the Service Management Manual.	Y	
R858.	7. In the case Malware is detected analyze Malware to determine the following:	Y	
R859.	7.1. Function of Malware	Y	
R860.	7.2. Infection vector of the Malware	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R861.	8. Develop methods using approved Tools, and/or work with appropriate approved vendors to provide enhanced detection and prevention processes.	Y	
R862.	9. Determine what if any data was/is compromised due to the security event. Include identified information in the security incident report.	Y	
R863.	10. Submit new Malware (zero-day) binaries to the anti-virus vendor for inclusion in the next pattern release.	Y	
R864.	11. Submit malicious URLs to Web security vendor to be classified as malicious.	Y	
R865.	12. Provide real-time Malware monitoring at Internet access points, using Tools to pull binaries from the live Internet stream. Actions performed on binaries include reverse engineering and exploding Malware in supported operating systems and/or as defined in the Service Management Manual.	Y	
R866.	13. Monitor DNS traffic for DNS requests to known malicious Internet addresses, interrogate URL and check for Malware, phishing, and any other malicious activity.	Y	
R867.	14. Provide the ability to re-route traffic to a central location and run the traffic through the real-time Malware monitoring Tools.	Y	
R868.	15. Assess the scope of damage related to all Malware events.	Y	
R869.	16. Arrest the spread and progressive damage from the Malware.	Y	
R870.	17. Eradicate Malware through techniques such as reverse engineering, custom scripting in endpoint management system, and working with the anti-virus vendor.	Y	
R871.	18. When recovering from a Malware compromise restore all data and Software to its original state.	Y	
R872.	19. Document troubleshooting steps that can be used by field associates to respond to Malware outbreaks or product issues.	Y	
R873.	20. Provide or use advanced Tools, including disassemblers, debuggers, tcpdump, and others as required.	Y	
R874.	21. Provide capability to scan for Malware upon demand using vendor-supplied scan methods and custom scan methods.	Y	
R875.	22. Respond to and support the Security Incident response processes.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R876.	23. Provide proactive alerts for consumption by End Users regarding current threats in the Customer Environment or based on industry information.	Y	
R877.	24. Provide daily, weekly, monthly and quarterly reports in the Security Dashboard on Malware infections and remediation.	Y	
R878.	25. Develop custom interface services, using standard APIs including those identified in the Service Management Manual, between approved anti-virus products and compliance, reporting and deployment Applications.	Y	
R879.	26. Develop interfaces using standard APIs including those identified in the Service Management Manual to provide a standard interface for other Tools to gather Malware detection data in an automated fashion.	Y	
R880.	27. Monitor anti-virus logs to detect any Malware infections.	Y	
R881.	28. Monitor logs from Web filtering, firewall, anti-virus and proactive Malware Tools for Malware infections and possible zero-day infections.	Y	
R882.	29. Integrate and manage event logging in to the SIEM infrastructure in accordance with the Service Management Manual.	Y	
R883.	30. Develop standard and custom reports to assist in Incident inquiry, correlation and response activities.	Y	
R884.	31. Perform correlation activities to identify ongoing threats based on data and reports from VITA, Customer, Supplier, authorized third parties and industry sources.	Y	
R885.	32. Develop installation instructions for the anti-virus solution.	Y	
R886.	33. Author knowledge base articles, integrating into Systems used by the End User Support and systems support personnel.	Y	
R887.	34. Maintain license and support compliance for the anti-virus product.	Y	
R888.	35. Maintain approved anti-virus exclusions ensuring proper alignment with vendor recommendations, technology best practices, and consultation with appropriate subject matter experts.	Y	
R889.	36. Maintain an auditable approval process for anti-virus exclusions ensuring proper alignment with all applicable security policies.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R890.	37. Audit and report on anti-virus exclusions quarterly, including contacting the exclusion requester to validate that the need for the exclusion still exists.	Y	
R891.	38. Include in the quarterly report the number of exclusions, number of new exclusions, number of exclusions removed and business justification for all exclusions.	Y	
R892.	39. Rapidly deploy anti-virus component updates during critical Security Events, as Directed by applicable security teams and policies.	Y	
R893.	40. Provide data and ad-hoc reporting to assist with forensics.	Y	
R894.	41. Develop custom scripts to assist in Malware remediation and detection.	Y	
R895.	42. Develop a process to address Malware protection requirements that are not provided by deployed anti-virus products in the Environment.	Y	
R896.	43. Provide the ability to discover and eradicate suspicious files based on hashes, file names, registry entries, paths, etc.	Y	
R897.	44. Provide the ability to blacklist or whitelist files based on names and/or hashes.	Y	
R898.	45. Provide standard and ad hoc reports from the solution that can be used for remediation, cleansing and correlation.	Y	
R899.	46. Provide analysis and recommendations from data, advising on corrective course of action.	Y	
R900.	47. Provide pro-active alerts to indicate potential virus activity based on definable triggers and rule sets.	Y	
R901.	48. Proactively compare data from system to Malware sites for hash verification of known Malware.	Y	
R902.	49. Provide web portal allowing remote execution of multiple anti-virus engines on assets and deliver scan results back to the centralized data repository.	Y	
R903.	50. Provide dedicated Malware technology to detect and alert for Malware attacks at the network perimeter.	Y	
R904.	51. Provide a solution that can analyze encrypted traffic where authorized by VITA and specified within the Service Management Manual.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R905.	52. Integrate and manage event logging in to the SIEM infrastructure in accordance with the Service Management Manual.	Y	
R906.	**3.3.4 Full Packet Capture**		
R907.	*This section identifies requirements for full packet capture.* *Supplier's responsibilities include:*		
R908.	1. Supplier will ensure that data is coming in at line speed and that there will be no delays with the system performance.	Y	
R909.	2. Supplier will verify that the system is capable to process the amount of data with ability to expand.	Y	
R910.	3. Supplier will provide a full packet capture solution can display collected data quickly. There will be significant number of events coming through, so the amount of time it takes to drill into them and get the information needed is important.	Y	
R911.	4. Supplier will provide a full packet capture solution that can easily be viewed by protocol, MAC, VLAN, geo-IP, and so on, and that data can be filtered.	Y	
R912.	5. Supplier will provide a full packet capture solution that has the ability to perform network behavior analysis (NBA) and block traffic that doesn't meet a certain policy.	Y	
R913.	6. Full packet capture solution provided by Supplier will have the ability to download sample packets for inspection using a protocol analyzer if needed, or if it will send them over to the authorities in accordance with the Service Management Manual.	Y	
R914.	7. Full packet capture solution will have the ability to retain and preserve the original timestamps. Timestamps will be synchronized to a common time zone.	Y	
R915.	8. Supplier will ensure that full packet capture solution will not cause a single point of failure.	Y	
R916.	9. Supplier will ensure that logs are saved and preserved.	Y	
R917.	10. Supplier will ensure the security of the packet capture solution.	Y	
R918.	11. Supplier will be aware of privacy concerns regarding full-packet capture. Supplier will be familiar with and review the relevant privacy laws.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R919.	12. Supplier will decrypt captured traffic when approved by VITA and in accordance with the Service Management Manual.	Y	
R920.	**3.3.5 Data Loss Prevention**		
R921.	*Supplier will provide a tool or system to monitor and filter data moving across Customer's network and creating an audit trail of policy-violation incidents. Supplier will monitor customer 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.* *Supplier's responsibilities include:*		
R922.	1. Provide a highly scalable solution capable of automatically detecting or blocking transmissions containing sensitive data, encrypting emails containing sensitive data, or quarantining messages that may need approval to exit Customer's network.	Y	
R923.	2. Provide a solution that is not limited to individual packets. The solution will decrypt captured information and intelligently assemble traffic streams into Application-layer sessions.	Y	
R924.	3. Provide a solution that is able to understand, reassemble and review various protocols such as SMTP, HTTP, HTTPS, Instant Message, FTP, Telnet, P2P communications and applications. Network DLP will support the reassembly and investigation of Microsoft Word, Microsoft Excel, and Adobe PDF attachments.	Y	
R925.	4. Provide a solution able to add additional scanning categories and content filters (e.g., adult content, credit card information, backdoors, key logger, P2P, personal information, Social Security numbers, violent acts).	Y	
R926.	5. Provide a solution able to define shared variables to be used by rules. This may include network address ranges, strings for pattern matching, etc.	Y	
R927.	6. Provide solution able to create custom signatures using pattern matching in conjunction with other defined rule parameters as specified in the Service Management Manual.	Y	
R928.	7. Evaluate network architecture, traffic patterns, protected system types and Customer DLP requirements to define custom rules and monitoring.	Y	
R929.	7.1. Using "out-of-the-box" policy and signature settings are not acceptable.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R930.	8. Coordinate with Customer and service providers to evaluate changes to network architecture, traffic patterns, protected system types and updated Customer security requirements at a minimum annually.	Y	
R931.	8.1. Provide a report to Customer summarizing the discussion and next steps.	Y	
R932.	9. Provide experienced technical contacts to support development and implementation Customer custom rule requests.	Y	
R933.	10. Respond to requests to provide detailed listings of all rules and logic.	Y	
R934.	11. Respond to requests to research and identify rule capabilities related to Customer perceived threats (e.g. new patch, internal investigation).	Y	
R935.	12. Conduct, in accordance with Customer's security policies, annual security scans of attached data storage at Customer facilities to look for sensitive data.	Y	
R936.	13. Provide the capability for data to be scanned at Customer facilities.	Y	
R937.	14. Provide the capability to scan for sensitive data upon demand for any device located on Customer's network.	Y	
R938.	15. Provide the ability to scan UNIX, Linux and Windows computers, file shares, servers, databases, repositories such as SharePoint and any other systems identified in the Service Management Manual.	Y	
R939.	16. Provide the capability to add additional domestic and international regulatory classifications to scanning criteria.	Y	
R940.	17. Provide the ability to throttle the host's CPU utilization during scanning, such that scanning is non-impacting to production systems and Applications.	Y	
R941.	18. Conduct scans as directed by VITA and/or Customer.	Y	
R942.	19. Provide continuous monitoring of scan progress to ensure that it is successfully completed.	Y	
R943.	20. Supplier's tool should provide the ability to export scan results.	Y	
R944.	21. Supplier and tool should provide analysis of exported scan results.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R945.	22. Communicate the scan results and remediation options with VITA and/or the data owning agency.	Y	
R946.	23. Provide "per scan" metrics on file deletion, file redaction, and file encryption and false positives.	Y	
R947.	24. Provide online analysis and reporting of the remediation efforts to include "per scan" metrics on file deletion, file redaction, and file encryption and false positives.	Y	
R948.	25. Provide Customer with the trends and progress reports as listed below:	Y	
R949.	25.1. Monthly, quarterly and yearly metrics of all scans conducted to include scan dates, name of server or shares, total number of Incidents, number of file deletions, number of file redactions, number of file encryptions, number of false positives across all content policies, and any other metrics specified in the Service Management Manual.	Y	
R950.	26. Provide the ability for requesting scan reports upon demand.	Y	
R951.	27. Manage the validation scanning and Application configuration to remove false positives.	Y	
R952.	28. Integrate and manage event logging in to the SIEM infrastructure in accordance with the Service Management Manual.	Y	
R953.	**3.3.6 Compliance Management**		
R954.	Supplier will participate in the compliance management program established for the environment. This participation may require deployment, implementation, and configuration of Supplier services in order to provide for support the compliance management program. The supplier may be required to take steps such as deploy software, modify configuration, integrate with a tool, etc. to support the compliance management program.	Y	
R955.	**3.3.7 Vulnerability Management**		
R956.	Supplier will participate in the vulnerability management program established for the environment. This participation may require deployment, implementation, and configuration of Supplier services in order to provide support for the vulnerability management program. The Supplier may be required to take steps such as deploy software, modify configuration, integrate with a tool, etc. to support the vulnerability management program.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R957.	**3.3.8 Penetration Testing**		
R958.	Supplier will participate in the penetration testing program established for the environment. The penetration testing program will require participation where identified and following procedures and requirements included in the Service Management Manual. All Suppliers will make services associated with this program available within the scope of the penetration testing program.	Y	
R959.	**3.3.9 Managed Firewall**		
R960.	*Supplier is responsible for all Enterprise (e.g., perimeter, core) and Non-Enterprise (e.g., departmental, local office) Firewalls (excluding end user). This section has some duplicated requirements from the perimeter network. Supplier will offer services for configuration, monitoring, change management, and support of firewall systems at designated facilities regardless of system and software ownership.* *Supplier's responsibilities include:*		
R961.	1. Provide and configure a secure multi-layer high availability firewall infrastructure with no single point of failure to support the Supplier and Program environment.	Y	
R962.	2. Where specified use different approved firewall manufacturers on separate layers to reduce exposure to any single manufacturer's exploit.	Y	
R963.	3. Ensure Firewalls have no negative impact on Network performance.	Y	
R964.	4. Integrate with the Change Management process approved by VITA and VITA Customers for the updating of firewall rules and objects, and obtain proper approvals prior to any revision.	Y	
R965.	5. Manage and update the firewall rules and objects as required.	Y	
R966.	6. Provide capability and process to expedite firewall rule change requests.	Y	
R967.	7. Respond to incidents and problems with Firewall Services.	Y	
R968.	8. Continuously monitor firewalls, and report any alerts or events to VITA and VITA Customers immediately, in accordance with the Service Management Manual, Customer's escalation and reporting procedures.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R969.	9. Provide program wide and individual Customer firewall rule set reports and configuration information via real time reporting and immediately upon request.	Y	
R970.	10. Integrate with MSI to provision Firewall Service Requests through online tools	Y	
R971.	11. Install, update, upgrade, patch, operate and maintain firewall protection Software and Systems in accordance with VITA and VITA Customer security requirements for all Software and Equipment in the environment.	Y	
R972.	12. Understand, maintain, and engineer the architecture of the solution to integrate into the identified environment.	Y	
R973.	13. Include recommendations for a host based firewall security profile.	Y	
R974.	14. Create and engineer security profiles and baselines for firewall systems.	Y	
R975.	15. Administer, configure, customize and test “out-of-the-box” firewall rules that have been identified applicable for a firewall security implementation.	Y	
R976.	16. Build firewall rules that will not disrupt business, while providing a secure platform.	Y	
R977.	17. Develop firewall rules which are used to identify and where specified block Malware or insecure Applications within Customer’s network. The required data for the rule may be derived from reverse engineering of Malware as well as industry security information and other threat intelligence data. Engineer firewall rules that can be used to alert on malicious traffic from within the infrastructure.	Y	
R978.	18. Configure firewall rules so to fit into business Application models while protecting against emerging threats.	Y	
R979.	19. Create firewall rule(s) as required by security threats, vulnerabilities, and industry best practices	Y	
R980.	20. Install and test rule updates that address known vulnerabilities or risks to endpoint systems, after such updates are identified by the vendor.	Y	
R981.	21. Ensure that the firewall rules created will not interfere with the function and operations of the environment.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R982.	22. Work with customers, following established change control policies, to test and validate firewall rules.	Y	
R983.	23. Install configuration updates to the systems as needed or directed, in accordance with the following;	Y	
	23.1. All changes must be tested on a test, development, or appropriate systems prior to implementation.	Y	
	23.2. Supplier must have intimate knowledge of Customer deployed assets and Applications to minimize possible risk to enterprise Applications.	Y	
R984.	24. Audit all firewall rules that have been created in response to security threats and business continuity at least quarterly, for their technical relevancy and integrity.	Y	
R985.	25. Ensure that firewall components are performing within defined performance guidelines and assist in all performance troubleshooting and testing activities.	Y	
R986.	26. Provide access to reports that will reflect on demand, daily, weekly, monthly status of overall firewall operational and rule data.	Y	
R987.	27. Develop remediation methods for devices that are missing firewall services within the Customer Environment.	Y	
R988.	28. Support exception handling processes and provide improvement recommendations to Customer or the Third Party Provider responsible for handling exception requests.	Y	
R989.	29. Maintain an auditable approval process for firewall rules ensuring proper alignment with all VITA and VITA Customer security policies and as established in the service management manual.	Y	
R990.	30. Maintain firewall rules ensuring proper alignment with recommendations, technology best practices, and consultation with subject matter experts.	Y	
R991.	31. Perform ongoing tuning of firewall system rules, security profiles, and configuration to minimize false positives and false negatives.	Y	
R992.	32. Review the firewall events (alarms) to identify false positives and systems that need remediation.	Y	
R993.	33. Remediate any of the systems that are in the error state and ensure that a firewall is installed and active.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R994.	34. Provide a method to submit endpoint firewall change requests.	Y	
R995.	35. Review new firewall change requests at least daily and as specified in the service management manual.	Y	
R996.	36. Integrate and manage logging of administrative actions in to the SIEM infrastructure in accordance with the service management manual.	Y	
R997.	37. Design and engineer a process or infrastructure that will allow the ability to audit and review all firewall rules as based off of the firewall request/exception process, and determine if the firewall rules are still valid, can be destroyed, or need to be updated.	Y	
R998.	37.1. Provide a portal and integration into a portal to allow Customers to review, approve, or identify for deletion firewalls rules impacting the customer and/or the enterprise.	Y	
R999.	38. The Supplier shall allow for penetration testing and vulnerability scans to be performed against the Solution.	Y	
R1000.	39. The Supplier shall ensure that the Operating System and other Patches should be applied in line with the SMM and VITA Rules.	Y	
R1001.	**3.3.9.1 Enclave**		
R1002.	*Supplier's responsibilities include:*		
R1003.	1. Provide network security services utilizing a defense-in-depth approach through enclaves (zoning) of the Enterprise network with multi-layered internal protections.	Y	
R1004.	2. Manage internal firewalls at the network level to enforce a security policy between tenants, and sub-tenants.	Y	
R1005.	3. Where identified manage firewalls to protect at the host level.	Y	
R1006.	4.		
R1007.	**3.4 End Point Security**		**Product Component (Answers may vary on requirements and applicable tools)**
R1008.	**3.4.1 Malware protection**		

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1009.	*This section identifies requirements for end points in the Managed Environment. These controls may extend to any device including, but not limited to servers, desktop, mobile devices, etc. This section also identifies requirements for managing anti-virus and other Malware protection software and systems in the environment regardless of ownership.* *Supplier will provide a Malware management security Tool to identify and protect Systems, data, devices and networks from Malware. This Tool will be provided to all Supplier's and designated third parties.* *Supplier's responsibilities include:*		
R1010.	5. Install, update, upgrade, patch, operate and maintain Malware Protection Software and systems in accordance with security requirements and VITA Rules for all Software and Equipment in the Environment, including all supported operating systems and platforms.	Y	Falcon Prevent
R1011.	6. Update anti-virus components on all devices within 24 hours of release and testing or in accordance with Service Management Manual and work with appropriate third-party vendors to immediately resolve issues.	Y	Falcon Prevent
R1012.	7. Verify that all anti-virus components are performing within documented performance characteristics and assist in all performance troubleshooting and testing activities.	Y	Atos personnel
R1013.	8. Understand Customer operating systems and Applications to effectively troubleshoot performance issues related to security products.	Y	Atos personnel
R1014.	9. Perform real-time Malware protection scanning in accordance with security requirements, VITA Rules, and the Service Management Manual.	Y	Falcon Prevent
R1015.	10. Perform scheduled scans of all Workstations and servers according to the Service Management Manual and VITA Rules. Monitor the status of the scans and remediate where necessary to avoid any performance or threat impact to the environment.	N	CrowdStrike (CS) does not support scheduled or on-demand scans, but it does continuously scan which obviates the need for scheduled or on-demand scans. Atomicorp Enterprise OSSEC ("AEO") supports scheduled and on-demand scans on the systems in which AEO is deployed.

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1016.	11. Upon detection of a Malware infection, respond immediately as defined by the Service Management Manual and VITA Rules.	Y	Falcon Prevent
R1017.	12. In the case Malware is detected, analyze Malware to determine the following:	Y	
R1018.	12.1. Function of Malware	Y	Falcon Prevent
R1019.	12.2. Infection vector of the Malware	Y	Falcon Prevent
R1020.	13. Develop methods using approved Tools, and/or work with appropriate approved Software vendors to provide enhanced detection and prevention processes.	Y	Atos personnel
R1021.	14. Determine what, if any, data was/is compromised due to the security event. Include identified information in the security incident report.	Y	Falcon Prevent
R1022.	15. Submit new Malware (zero-day) binaries to the anti-virus vendor for inclusion in the next pattern release.	Y	Falcon Prevent uses machine learning and AI to identify zero-day threats. These are reported to CrowdStrike.
R1023.	16. Submit malicious URLs to Web security vendor to be classified as malicious.	Y	Falcon Prevent uses machine learning and AI to identify threats. These are reported to CrowdStrike.
R1024.	17. Provide real-time Malware monitoring at Internet access points, using Tools to pull binaries from the live Internet stream. Actions performed on binaries include reverse engineering and exploding Malware in supported operating systems and/or as defined in the Service Management Manual and VITA Rules.	Y	Falcon Prevent works at the endpoint. Monitoring at Internet access points is accomplished by Palo Alto Threat Prevention, within the Internet firewall.
R1025.	18. Monitor DNS traffic for DNS requests to known malicious Internet addresses, interrogate URL and check for Malware, phishing, and any other malicious activity.	Y	Falcon Prevent
R1026.	19. Provide the ability to re-route traffic back to a central location and run the traffic through the real-time Malware monitoring Tools.	Y	All Falcon Prevent scanning is continuous and in real-time. Previously undetected threats are sent back to the CrowdStrike Cloud for further analysis.

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1027.	20. Assess the scope of damage related to all Malware events.	Y	Falcon Prevent
R1028.	21. Arrest the spread and progressive damage from the Malware.	Y	Falcon Prevent
R1029.	22. Eradicate Malware through techniques such as reverse engineering, custom scripting in endpoint management system, and working with the anti-virus vendor.	Y	Atos personnel and Falcon Overwatch
R1030.	23. When recovering from a Malware compromise restore all data and Software to its original state.	Y	Falcon Prevent prevents most malware attacks and cleans up any artifacts left behind by the attempt. In the case of actual compromise, Real Time Response is a dedicated remediation tool. Incident Responders can utilize this tool to completely remediate an endpoint without the need for a re-image.
R1031.	24. Document troubleshooting steps that can be used by field associates to respond to Malware outbreaks or product issues.	Y	Real Time Response is a dedicated remediation tool. Incident Responders can utilize this tool to completely remediate an endpoint without the need for a re-image.
R1032.	25. Provide or use advanced Tools, including disassemblers, debuggers, tcpdump, and others as required.	Y	Real Time Response is a dedicated remediation tool. Incident Responders can utilize this tool to completely remediate an endpoint without the need for a re-image.
R1033.	26. Provide capability to scan for Malware upon demand using vendor-supplied scan methods and custom scan methods.	N	CrowdStrike (CS) does not support scheduled or on-demand scans, but it does continuously scan which obviates the need for

Ref#	Requirement	Comply (Y/N)	Supplier Response
			scheduled or on-demand scans. Atomicorp Enterprise OSSEC ("AEO") supports scheduled and on-demand scans on the systems in which AEO is deployed.
R1034.	27. Respond to and support the Security Incident response processes.	Y	Atos personnel
R1035.	28. Provide proactive alerts for consumption by End Users regarding current threats in the Customer Environment or based on industry information.	Y	Falcon Insight and Overwatch
R1036.	29. Provide daily, weekly, monthly, and quarterly reports in the Security Dashboard on Malware infections and remediation activities.	Y	Atos personnel
R1037.	30. Develop custom interface services, using standard APIs (including those identified in the Service Management Manual), between approved anti-virus products and compliance, reporting and deployment Applications.	Y	Atos personnel
R1038.	31. Develop interfaces or use standard APIs (including those identified in the Service Management Manual), to provide a standard interface for other Tools to gather Malware detection data in an automated fashion.	Y	Atos personnel
R1039.	32. Monitor anti-virus logs to detect any Malware infections.	Y	Falcon Insight and AIsaac MDR
R1040.	33. Monitor logs from Web filtering, firewall, anti-virus and proactive Malware Tools for Malware infections and possible zero-day infections.	Y	Falcon Insight and AIsaac MDR
R1041.	34. Develop, maintain and administer a centralized data repository and reporting framework that consolidates information from dissimilar security products.	Y	AIsaac MDR and Security Dashboard
R1042.	35. Retain data in centralized repository online for a minimum of one year.	Y	
R1043.	36. Develop standard and custom reports to assist in Incident inquiry, correlation and response activities.	Y	Atos personnel
R1044.	37. Perform correlation activities to identify ongoing threats based on data and reports from VITA, Customer, Supplier, authorized third parties and industry sources.	Y	Atos personnel and AIsaac MDR
R1045.	38. Develop installation instructions for the anti-virus solution.	Y	Atos personnel

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1046.	39. Author knowledge base articles and integrate into Systems used by the End User Support and systems support personnel.	Y	Atos personnel
R1047.	40. Maintain license and support compliance for the anti-virus product(s).	Y	Atos personnel
R1048.	41. Maintain approved anti-virus exclusions ensuring proper alignment with vendor recommendations, technology best practices, and consultation with appropriate subject matter experts.	Y	Atos personnel
R1049.	42. Maintain an auditable approval process for anti-virus exclusions ensuring proper alignment with all applicable security policies.	Y	Atos personnel will support the process according to the relevant SMMs.
R1050.	43. Audit and report on anti-virus exclusions quarterly, including contacting the exclusion requester to validate that the need for the exclusion still exists.	Y	Atos personnel
R1051.	44. Include in the quarterly report the number of exclusions, number of new exclusions, number of exclusions removed, and business justification for all exclusions.	Y	Atos personnel
R1052.	45. Rapidly deploy anti-virus component updates during critical Security Events, as directed by applicable security teams, policies, and VITA Rules.	Y	Atos personnel
R1053.	46. Set up, monitor and troubleshoot backups of all anti-virus products.	Y	Atos personnel
R1054.	47. Provide data and ad-hoc reporting to assist with forensics.	Y	Falcon Insight and AIsaac MDR
R1055.	48. Develop custom scripts to assist in Malware remediation and detection.	Y	Atos personnel
R1056.	49. Develop a process to address Malware protection requirements that are not provided by deployed anti-virus products in the Environment.	Y	Atos believes Falcon Prevent will detect and prevent all unknown malware but Atos personnel will work with MSI to develop the appropriate process.
R1057.	50. Provide the ability to discover and eradicate suspicious files across the environment based on hashes, file names, registry entries, paths, etc.	Y	Falcon Prevent
R1058.	51. Provide the ability to blacklist or whitelist files based on names and/or hashes.	Y	Falcon Discover
R1059.	52. Provide standard and ad hoc reports from the solution that can be used for remediation, cleansing and correlation.	Y	Falcon Insight and Atos personnel

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1060.	53. Provide analysis and recommendations from collected data, advising on corrective course of action.	Y	Falcon Insight and Atos personnel
R1061.	54. Provide pro-active alerts to indicate potential virus activity based on definable triggers and rule sets.	Y	Falcon Prevent, Falcon Insight
R1062.	55. Proactively compare data from system to Malware sites for hash verification of known Malware.	Y	Falcon Prevent
R1063.	56. Provide web portal allowing remote execution of multiple anti-virus engines on assets and deliver scan results back to the centralized data repository.	Y	Falcon Prevent
R1064.	57. Provide dedicated Malware technology to detect and alert for Malware attacks, integrating with the other malware protection technologies deployed within the environment.	Y	Falcon Prevent
R1065.	58. Provide a solution that will support end points for Suppliers participating within the environment.	Y	Falcon Prevent supports Windows, Windows Server, macOS and Linux
R1066.	**3.4.2 Managed Host Intrusion Prevention**		
R1067.	*Supplier will provide a solution for configuration, monitoring, change management, and support of Host Intrusion Protection System (HIPS) software on end-point devices regardless of device and software ownership, including management of end-point software firewalls.* *Supplier's responsibilities include:*		Falcon Insight, Falcon Firewall Management
R1068.	59. Install, update, upgrade, patch, operate, and maintain the HIPS in accordance with security requirements and VITA Rules.	Y	Atos personnel
R1069.	60. Maintain up to date HIPS deployment locations, version identification, policy configuration, status overview, and any other requirements specified the Service Management Manual and VITA Rules and have that information available to VITA/Customer.	Y	Atos personnel
R1070.	61. Support the program exception process.	Y	Atos personnel
R1071.	62. Install HIPS updates and make configuration changes that address known vulnerabilities or risks; as such updates are identified by the vendor of the HIPS, suggested in	Y	Atos personnel

Ref#	Requirement	Comply (Y/N)	Supplier Response
	accordance with industry best practices, or as required to maintain compliance with security requirements.		
R1072.	63. Perform full production-mirroring testing validation for Customer-designated critical Systems as part of the Change Management process.	Y	Atos personnel
R1073.	64. Coordinate and actively participate for testing of the HIPS solution on all platforms and machine configurations.	Y	Atos personnel
R1074.	65. Create, develop, and maintain multiple policies to support devices identified within the environment.	Y	Atos personnel
R1075.	66. Provide quarterly reviews of policy components and signatures for each policy deployed to the HIPS. Make recommendations for signature and policy component updates. The report should contain:	Y	Atos personnel
R1076.	66.1. Resulting analysis and reporting from policy and architecture review performed by the Supplier.	Y	Atos personnel
R1077.	66.2. A summary discussion of new threats, trends, proactive discoveries by the Supplier.	Y	Atos personnel
R1078.	66.3. An accounting of signature settings active based on attack classification, operating system, and key systems.	Y	Atos personnel
R1079.	66.4. Provide research as needed to identify HIPS signatures related to perceived threats. This may result from a new patch or internal investigation.	Y	Atos personnel
R1080.	67. Provide a report, upon request, which clearly documents all policy components and signatures, activated and not activated.	Y	Atos personnel
R1081.	68. Define and develop a clear communication template that can be understood by non-security IT stakeholders. The template should be used and communicated with all escalated alerts and should include:	Y	Atos personnel
R1082.	68.1. A clear event summary, including analyst brief on the signature fired, the source, target systems, vector and attack type	Y	Atos personnel
R1083.	68.2. Summary of the threat matrix rating	Y	Atos personnel
R1084.	68.3. A descriptive analyst brief of the attack type as it relates to Customer exposure	Y	Atos personnel

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1085.	68.4. An analyst brief of impact – both received and possible impact	Y	Atos personnel
R1086.	68.5. An analyst brief of false positive analysis	Y	Atos personnel
R1087.	69. Develop alert escalation processes in accordance with the Service Management Manual and VITA Rules.	Y	Atos personnel
R1088.	70. Evaluate all alerts for threat level, possible impact, and false positives.	Y	Falcon Insight
R1089.	71. Communicate alerts using the defined alert communication template and threat matrix as defined above and in the Service Management Manual and VITA Rules.	Y	Atos personnel
R1090.	72. Maintain relationships and contacts with other Third Party security resources that may be used to identify additional attack mitigation steps (e.g., Web Application firewall, ISPs, Packet Scrubbing).	Y	Atos personnel
R1091.	73. Define a process for approving the filtering of alerts. Alert filtering will be approved by VITA and documented according to the Service Management Manual and VITA Rules.	Y	Atos personnel
R1092.	**3.4.3 Managed Firewall**		
R1093.	*Supplier will provide a solution for configuration, monitoring, change management, and support of firewall systems for end points at Customer designated facilities regardless of system and software ownership.* *Supplier's responsibilities include:*		Falcon Firewall Management
R1094.	74. Install, update, upgrade, patch, operate and maintain firewall protection Software and Systems in accordance with security requirements and VITA Rules for all Software and Equipment in the environment.	Y	Atos personnel
R1095.	75. Understand, maintain, and engineer the architecture of the solution.	Y	Atos personnel
R1096.	76. Include recommendations for a host-based firewall security profile.	Y	Atos personnel
R1097.	77. Create and engineer security profiles that contain a firewall module, to be used on Customer network end points, including client-based Workstations and server OS.	Y	Atos personnel
R1098.	78. Administer, configure, customize and test "out-of-the-box" firewall rules that have been identified applicable for a firewall security implementation.	Y	Atos personnel
R1099.	79. Build firewall rules that will not disrupt business, while providing a secure platform.	Y	Atos personnel

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1100.	80. Develop firewall rules which are used to identify Malware or insecure Applications within Customer's network. The required data for the rule is derived from reverse engineering of Malware and industry security information. Engineer firewall rules that can be used to alert on malicious traffic from client-based Workstations and key server infrastructures.	Y	Atos personnel
R1101.	81. Configure firewall rules so to fit into business Application models while protecting against emerging threats as they become known.	Y	Atos personnel
R1102.	82. Create firewall rule(s) as required by security threats, vulnerabilities, and industry best practices:	Y	Atos personnel
R1103.	82.1. If a new threat (such as compromised devices or unauthorized and unmanaged software with a critical vulnerability) is discovered within the environment, write rules to secure the environment.	Y	Atos personnel
R1104.	82.2. Monitor custom rule deployment and address any of the ad-hoc troubleshooting or maintenance requests immediately.	Y	Atos personnel
R1105.	83. Ensure that the firewall rules cover the operating systems and Applications in the environment.	Y	Atos personnel
R1106.	84. Install and test rule updates that address known vulnerabilities or risks to endpoint systems, after such updates are identified by the vendor.	Y	Atos personnel
R1107.	85. Ensure that the firewall rules created will not interfere with the function and operations of the environment.	Y	Atos personnel
R1108.	86. Work with customers, following established change control policies, to test and validate firewall rules.	Y	Atos personnel
R1109.	87. Install configuration updates to the endpoint systems as needed or directed, in accordance with the following;	Y	Atos personnel
R1110.	87.1. All changes will be tested on a test, development or appropriate systems prior to implementation.	Y	Atos personnel
R1111.	87.2. Supplier will have intimate knowledge of Customer deployed assets and Applications to minimize possible risk to VITA, Customer and other Supplier Applications.	Y	Atos personnel

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1112.	88. Audit all firewall rules that have been created in response to security threats and business continuity at least quarterly, for their technical relevancy and integrity.	Y	Atos personnel
R1113.	89. Ensure that firewall components are performing within defined performance guidelines and assist in all performance troubleshooting and testing activities.	Y	Atos personnel
R1114.	90. Provide to Customer and routinely review reporting metrics indicating number of systems that:	Y	Atos personnel
R1115.	90.1. Should use host-based firewall solution	Y	Atos personnel
R1116.	90.2. Are protected using a host-based firewall solution	Y	Atos personnel
R1117.	90.3. Systems that are not using a host-based firewall (offline systems)	Y	Atos personnel
R1118.	91. Provide on demand access to reports that reflect the daily, weekly, and monthly status of overall firewall operational and rule data.	Y	Atos personnel
R1119.	92. Develop remediation methods for devices that are missing firewall services within the Customer Environment.	Y	Atos personnel
R1120.	92.1. Identify the ownership of the end point device.	Y	Atos personnel
R1121.	92.2. Coordinate with owner a time for investigation for firewall services that are offline.	Y	Atos personnel
R1122.	92.3. Schedule a ‘system change’ to take action on the end point that is offline once a solution has been identified.	Y	Atos personnel
R1123.	92.3.1. System changes should be understood that prior notice is given to end point owner, unless otherwise identified as a security risk.	Y	Atos personnel
R1124.	92.3.2. System changes are to take place after business hours in the time zone of the end point, unless otherwise identified as a security risk.	Y	Atos personnel
R1125.	93. Support exception handling processes and provide improvement recommendations to Customer or the Third Party Provider responsible for handling exception requests.	Y	Atos personnel
R1126.	94. Maintain an auditable approval process for firewall rules ensuring proper alignment with all security policies, VITA Rules, and as established in the Service Management Manual.	Y	Atos personnel

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1127.	95. Maintain firewall rules ensuring proper alignment with recommendations, technology best practices, and consultation with subject matter experts.	Y	Atos personnel
R1128.	96. Perform ongoing tuning of firewall system rules, security profiles, and configuration to minimize false positives and false negatives.	Y	Atos personnel
R1129.	97. Ensure that the host firewall solution supports all operating systems and major Applications defined by Customer, including Windows, Linux, HP-UX, AIX, Oracle, WebSphere, Apache, IIS, SQL Server or others as defined in the Service Management Manual.	Y	
R1130.	98. Provide standard and ad-hoc reports for Customer that include the following:	Y	Atos personnel
R1131.	98.1. Number of devices installed	Y	Atos personnel
R1132.	98.2. Number of devices failed	Y	Atos personnel
R1133.	98.3. Health status:	Y	Atos personnel
R1134.	98.3.1. Online for firewall	Y	Atos personnel
R1135.	98.3.2. Offline for firewall	Y	Atos personnel
R1136.	99. Review the firewall events (alarms) to identify false positives and systems that need remediation.	Y	Atos personnel
R1137.	100. Remediate any of the systems that are in the error state and ensure that a firewall is installed and active.	Y	Atos personnel
R1138.	101. Provide a method to submit endpoint firewall change requests.	Y	Atos personnel
R1139.	102. Review new firewall change requests at least daily and as specified in the Service Management Manual and VITA Rules.	Y	Atos personnel
R1140.	103. Design and engineer a process or infrastructure that will allow the ability to audit and review all firewall rules as based off of the firewall request/exception process, and determine if the firewall rules are still valid, can be destroyed, or need to be updated.	Y	Atos personnel

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1141.	103.1. Provide a portal to allow VITA/Customers to review, approve, or identify for deletion firewalls rules impacting the customer and/or the program-wide environment.	Y	Security Dashboard
R1142.	**3.4.4 Data Loss Prevention**		
R1143.	*The Supplier will be responsible for providing a tool to perform endpoint data loss prevention. Supplier's responsibilities include:*		
R1144.	104. Provide, deploy, install, implement, configure, maintain and administer a VITA-approved tool capable of monitoring real time end user activity.	Y	
R1145.	105. The tool will be able to apply centrally managed security policies.	Y	
R1146.	106. The tool will be able to regulate and restrict access to sensitive data according to customer's data classification.	Y	
R1147.	107. The tool will be able to provide instant responses to persisting threats and prevent data from being exfiltrated.	Y	
R1148.	108. Provide comprehensive protection for all potential leaking channels, to include removable storage devices, cloud, email, instant messenger, clipboard, printing, screen capture, etc.	Y	
R1149.	109. The tool will be able to perform discovery scans and perform self-remediation actions.	Y	
R1150.	110. The tool will be centrally managed and be capable of reporting incidents, and provide continuous monitoring and auditing capabilities.	Y	
R1151.	111. The tool will support role-based access control to enforce separation of duties.	Y	
R1152.	112. The tool will produce regulatory compliance measures reports.	Y	
R1153.	**3.4.5 Reserved**		
R1154.			
R1155.	113.		
R1156.	114.		
R1157.	115.		

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1158.	**3.4.6 Endpoint Application/Process Whitelisting**		
R1159.	*The Supplier will be responsible for providing a solution to centrally manage the endpoint applications and process authorization.* *Supplier's responsibilities include:*		
R1160.	116. Solution will provide real time monitoring.	Y	
R1161.	117. Solution will support performing an initial discovery phase to determine authorized applications/processes at the endpoint.	Y	
R1162.	118. Solution will provide alerts for applications/processes that were not authorized for use.	Y	
R1163.	119. Solution will be capable of notifying designated parties for approval of applications/processes that are not part of the established environment baseline.	Y	
R1164.	120. Solution will run seamlessly at the endpoint to automatically check against the authorized list of processes when a process is executing.	Y	
R1165.	121. Solution will perform an integrity check such as hashing to ensure the application/process is in fact the authorized application/process and not a malicious or otherwise inappropriate application with the same executable name.	Y	
R1166.	122. Solution will prevent unauthorized processes from executing.	Y	
R1167.	123. Solution will report activity to the SIEM and identified log collection points.	Y	
R1168.	124. Solution will support multiple policies/profiles that include combinations of process blocking and allowing process execution.	Y	
R1169.	125. Solution will support all software deployed within the environment.	Y	
R1170.	**3.4.7 Endpoint File Integrity Check**		
R1171.	*Supplier's responsibilities include:*		
R1172.	126. Solution will provide a searchable interface that contains all locations where a data asset using the endpoint file integrity check system is stored.	Y	Falcon Discover
R1173.	127. Solution will provide for a multi-tenant environment where each agency can view only their information and VITA can view the program-wide environment information.	Y	Falcon Discover
R1174.	128. Create a baseline of the Customer's environment.	Y	Falcon Discover

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1175.	129. Solution will, at a minimum, provide a list of the file names, hash value (using a VITA approved hash algorithm) and time stamp.	Y	Falcon Discover
R1176.	130. Solution will have the ability to check all files, processes, and system information on a device.	Y	Falcon Discover
R1177.	131. Alert on registry changes, file changes, and other system related changes.	Y	Falcon Discover
R1178.	132. Provide an activity report to view a full timeline of file activity.	Y	Falcon Discover
R1179.	133. Monitor files for tampering, modifications, and deletions as well as permission changes.	Y	Falcon Discover
R1180.	134. Provide real time notification of changes made to files, folders and registry settings.	Y	Falcon Discover
R1181.	135. Correlate with Directory Services to obtain information on the users responsible for changes.	Y	Atos Personnel
R1182.	136. Solution will integrate into the monitoring and logging solution.	Y	Falcon Discover
R1183.	137. Solution will allow custom configuration in a multi-tenant environment to monitor user identified files, processes, and system information.	Y	Falcon Discover
R1184.	**3.4.8 Compliance Management**		
R1185.	Supplier will participate in the compliance management program established for the environment. This participation may require deployment, implementation, and configuration of Supplier services in order to provide support for the compliance management program. The supplier may be required to take steps such as deploy software, modify configuration, integrate with a tool, etc. to support the compliance management program.	Y	
R1186.	**3.4.9 Vulnerability Management**		
R1187.	Supplier will participate in the vulnerability management program established for the environment. This participation may require deployment, implementation, and configuration of Supplier services in order to provide support for the vulnerability management program. The Supplier may be required to take steps such as deploy software, modify configuration, integrate with a tool, etc. to support the vulnerability management program.	Y	
R1188.	**3.4.10 Penetration Testing**		

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1189.	Supplier will participate in the penetration testing program established for the environment. The penetration testing program will require participation where identified and following procedures and requirements included in the Service Management Manual and VITA Rules. All Suppliers will be expected to make services associated with this program available to be within the scope of the penetration testing program.	Y	
R1190.	**3.4.11 Full Disk Encryption (Attached Device)**		
R1191.	*Supplier's responsibilities include:*		
R1192.	138. The encryption system will support the existing multi factor authentication solution.	Y	
R1193.	139. The encryption system will utilize the existing infrastructure.	Y	
R1194.	140. The encryption system should allow multiple users to access an encrypted device.	Y	
R1195.	141. The encryption system should support various authentication methods to include but not limited to common biometric identification hardware, passwords, USB tokens, smart cards.	Y	
R1196.	142. The encryption system will be capable of allowing an authorized administrator without an account on the system to decrypt the device.	Y	
R1197.	143. The encryption system will support the ability to perform a forensic analysis of the encrypted data. The device will be able to be decrypted within the forensic software to support the forensic analysis.	Y	
R1198.	144. The encryption system will integrate with the existing system logon process during authentication.	Y	
R1199.	145. The encryption system will directly authenticate to the existing authentication services, with the capability to, authenticate with a local account.	Y	
R1200.	146. The encryption system will encrypt the entire hard drive including temporary, swap files, and hibernation files.	Y	
R1201.	147. The encryption system will use industry recognized secure algorithms with a minimum of a 256-bit key capability.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1202.	148. The encryption system will be transparent to the end user.	Y	
R1203.	149. Only authorized personnel will be capable of removing or disabling the encryption Software.	Y	
R1204.	150. The encryption system must not interfere with user's productivity.	Y	
R1205.	151. The encryption system will have the capability to encrypt media and devices attached to the encrypted device.	Y	
R1206.	152. The encryption system will support the environments device provisioning and de-provisioning process.	Y	
R1207.	153. The encryption system provide protection during boot up.	Y	
R1208.	**3.5 Application Security**		
R1209.	**3.5.1 Source Code Scanning**		
R1210.	*Application Security controls focus on applying security measures that impact applications. The controls are intended to provide additional security for circumstances when the security controls are needed, as well as when there are compensating controls required. Supplier will provide a solution for VITA Customers to:*		
R1211.	1. Examine application source code and/or compiled source code to detect and report flaws that can lead to security vulnerabilities including the OWASP Top Ten	Y	
R1212.	2. Solution will be capable of scanning multiple development languages including but not limited to .NET. C, C++, Java, etc.	Y	
R1213.	3. Solution will be capable of scanning the integrated development environment and provide immediate feedback during the software development phase	Y	
R1214.	4. Application source code will be scanned before deployment into production and after release into production on a quarterly basis or after a significant application change	Y	
R1215.	5. Supplier will provide customer with a detailed report of scan results showing criticality, results and mitigation recommendations	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1216.	6. Provide source code scanning reports on demand or quarterly in accordance with the Service Management Manual.	Y	
R1217.	**3.5.2 Vulnerability Scanning**		
R1218.	*This section identifies requirements for scanning of particular devices and subnets for known vulnerabilities.* *Supplier's responsibilities include:*		
R1219.	1. Pre-Production.	Y	
R1220.	1.1. Scan any applicable new Systems, devices, or any Systems to be deployed in a new project. Scans will include an operating system scan, a web vulnerability scan for Web servers, and any other applicable scan types identified in the Service Management Manual.	Y	
R1221.	1.2. Once any vulnerabilities have been addressed, rescan the system and notify the owner of the results.	Y	
R1222.	1.3. Ensure that no System is moved into production until any identified vulnerability is corrected or an exception has been granted.	Y	
R1223.	1.4. Conduct pre-production consulting with the teams responsible for the assets in question on an ad-hoc basis.	Y	
R1224.	2. Production		
R1225.	2.1. Perform security vulnerability assessments in accordance with security requirements.	Y	
R1226.	2.2. Document and communicate the scan results and recommend remediation activities to reduce security risks.	Y	
R1227.	2.3. Coordinate and track to completion any remediation tasks related to any vulnerabilities discovered.	Y	
R1228.	2.4. Perform scheduled vulnerability scans as required by policy, statute, federal requirements and VITA Rules.	Y	
R1229.	2.5. Review scan results and identify the vulnerabilities which require remediation.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1230.	3. Application Scanning	Y	(Application Scanning suspended on MOD 23 Effective Date)
R1231.	3.1. Scan Applications as requested by Customer in order to evaluate, test and recommend security maintenance activities including upgrades, patches, and fixes.	Y	(Application Scanning suspended on MOD 23 Effective Date)
R1232.	3.2. Work with the Application's owner or external vendor to remediate Application scan vulnerability issues.	Y	(Application Scanning suspended on MOD 23 Effective Date)
R1233.	3.3. Scan Web Applications on a frequency defined by the Service Management Manual.	Y	(Application Scanning suspended on MOD 23 Effective Date)
R1234.	3.4. Web application scans should be completed using an approved tool designed for web application scanning.	Y	(Application Scanning suspended on MOD 23 Effective Date)
R1235.	4. Network Scanning	Y	
R1236.	4.1. Scan network devices in order to identify any deviations from specified configurations, misconfigurations, or device vulnerabilities.	Y	
R1237.	5. Vulnerability Scanning Reporting.	Y	
R1238.	5.1. Report detected vulnerabilities and non-compliance issues as defined in the Service Management Manual.	Y	
R1239.	5.2. Provide an updated vulnerability scan report once every calendar month.	Y	
R1240.	5.3. Report will be available via a portal that allows filtering on required reporting areas.	Y	
R1241.	5.4. Vulnerability scan report will at a minimum include the following fields. The report should be able to sort on each field.	Y	
R1242.	5.4.1. The target IP address	Y	
R1243.	5.4.2. The vulnerabilities discovered	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1244.	5.4.3. CVSS scores and the CVE and where applicable CWE of the vulnerabilities discovered	Y	
R1245.	5.4.4. Severity level of vulnerabilities discovered	Y	
R1246.	5.4.5. Description of vulnerability	Y	
R1247.	5.4.6. Affected software, firmware, and/or hardware	Y	
R1248.	5.4.7. Indication of whether the vulnerability is confirmed by the tool or is a potential vulnerability	Y	
R1249.	5.4.8. Vulnerability identifiers	Y	
R1250.	5.4.9. List of the target's open ports	Y	
R1251.	5.4.10. Host information such as device name, MAC address, NetBIOS name, etc.	Y	
R1252.	5.5. Each vulnerability scan report will include corresponding recommendations for remediation.	Y	
R1253.	5.6. Supplier will work with the owner of vulnerable system to advise, complete, and develop remediation plans and take any approved steps necessary to correct the issue.	Y	
R1254.	**3.5.3 Web Application Firewall**		
R1255.	*Supplier will provide a multi-tenant, high availability, scalable web application firewall (WAF) solution for Customer web applications that will protect from web based attacks by external threat actors.* *Supplier's responsibilities include:*		
R1256.	1. Solution will protect against attacks such as those included in the OWASP Top Ten, DDoS attacks, etc.	Y	
R1257.	2. Solution will provide inspection and detection of encrypted web application traffic. If any malicious traffic is detected, it will trigger an alert for investigation.	Y	
R1258.	3. The Supplier will coordinate with the Customer to customize WAF security profiles for custom applications.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1259.	4. Solution provide server cloaking protection to prevent exposure of web server infrastructure details and block web scraping attacks.	Y	
R1260.	5. Solution will export audit logs to the SEIM solution.	Y	
R1261.	**3.5.4 Compliance Management**		
R1262.	Supplier will participate in the compliance management program established for the environment. This participation may require deployment, implementation, and configuration of Supplier services in order to provide support the compliance management program. The Supplier may be required to take steps such as deploy software, modify configuration, integrate with a tool, etc. to support the compliance management program.	Y	
R1263.	**3.5.5 Vulnerability Management**		
R1264.	Supplier will participate in the vulnerability management program established for the environment. This participation may require deployment, implementation, and configuration of Supplier services in order to provide support the vulnerability management program. The Supplier may be required to take steps such as deploy software, modify configuration, integrate with a tool, etc. to support the vulnerability management program.	Y	
R1265.	**3.5.6 Penetration Testing**		
R1266.	Supplier will participate in the penetration testing program established for the environment. The penetration testing program will require participation where identified and following procedures and requirements included in the Service Management Manual. All Suppliers will be expected to make services associated with this program available to be within the scope of the penetration testing program.	Y	
R1267.	**3.5.7 Access Management**		
R1268.	*The following requirements are intended to support an identity and access management solution that integrates all Suppliers throughout the program environment. The services in the Access Management section may be provided by another Supplier, please ensure a solution is designed in a fashion that permits for the flexibility to incorporate Access Management from this Supplier or from another Supplier.* *Identity and Access Management (IAM) seeks to provide authoritative identification of users and to grant designated users the right to use a service, while preventing unauthorized access.*		Security Supplier assumes the MSI Supplier's Identity and Access Management (IAM) suite addresses these requirements. [R1268-R1333]

Ref#	Requirement	Comply (Y/N)	Supplier Response
	The Supplier will define, implement and operate IAM protocols, tools and processes across the Service Towers that enable access rights and identities to be established, controlled, authorized, administered, reported, and audited in adherence with the VITA Rules, Commonwealth policies, Commonwealth standards, and Customer requirements as maintained in the Service Management Manual. *Supplier's responsibilities include:*		
R1269.	1. Provide notification of suspicious or malicious account activity to the designated parties included in the SMM immediately upon discovery	N	
R1270.	2. Provide Systems and Tools which:		
R1271.	2.1. Provide capability to manage accounts (e.g. individually and in mass, provision, reactivate, modify, de-provision, suspend, etc.) in order to govern access.	N	
R1272.	2.2. Provide account management interoperability with third party applications. (i.e. APIs or Web services, scripting).	N	
R1273.	2.3. Provide for the capability to present a dashboard of account, role, monitoring information and any other relevant data, with multiple tiers of reporting and management access.	N	
R1274.	2.4. Provide for the capability to delegate the account management for individual Customers while maintaining centralized governance in accordance with the SMM.	N	
R1275.	2.5. Provide for the capability to prioritize account management functions.	N	
R1276.	2.6. Provide Customers with the capability to exercise authority for approval of all data and System access requirements.	N	
R1277.	2.7. Provide for capability to simultaneously fully integrate with industry-standard directory services (e.g., X.500, LDAP, Active Directory).	N	
R1278.	2.8. Provide a solution that includes single on capabilities which integrate with industry-standard directory services.	N	
R1279.	2.9. Provide the capability to manage privileged accounts.	N	

Ref#		Requirement	Comply (Y/N)	Supplier Response
R1280.	2.10.	Provide the capability for identity federation that supports all Federal Assurance Levels (FAL), as defined in NIST 800-63, with single sign-on (SSO) functionality.	N	
R1281.	2.11.	Provide for the capability to utilize the most current or version as identified in the SMM Security Assertion Markup Language (SAML), Oauth, and others as required by Systems Management Services.	N	
R1282.	2.12.	Provide for the capability for each Customer to perform on-demand access audits.	N	
R1283.	2.13.	Provide for the capability to create custom workflows and interfaces that can integrate with third party application APIs and web services using industry standard data formats.	N	
R1284.	2.14.	Provide the capability to log all account identity, access, and authorization activity and allow Customers to generate custom reports using this data.	N	
R1285.	2.15.	Provide the capability to log all system activity and generate custom reports using this data.	N	
R1286.	2.16.	Provide the capability to retain all log data generated by the solution in accordance with VITA Rules and the SMM and log all data to the identified centralized logging service.	N	
R1287.	2.17.	Provide the capability to support Role-based Access Control (RBAC), Access Control List (ACL), Organization-based access control, and Attribute-based Access Control (ABAC) models.	N	
R1288.	2.18.	Provide the capability to collect, monitor, alert and report on separation-of-duty access requirements for accounts as defined by the Customer.	N	
R1289.	2.19.	Provide the capability for temporary account provisioning, reactivation, modification, de-provisioning, suspension, and governance.	N	
R1290.	2.20.	Provide the capability to support Multifactor Authentication (MFA) which supports industry standards (e.g. PIV-I card standard).	N	
R1291.	2.21.	Provide the capability to clone or replicate access profiles, roles, and/or other classification identifiers with grouped attributes.	N	
R1292.	2.22.	Provide the capability of self-service for integration with third party applications.	N	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1293.	2.23. Provide the capability for behavioral and/or situational access controls including but not limited to time based restrictions and geo location restrictions.	N	
R1294.	2.24. Provide the capability to offer password vaulting for accounts.	N	
R1295.	2.25. Provide the capability for a self-service portal to provision, reactivate, modify, de-provision, suspend, and govern accounts.	N	
R1296.	2.26. Provide the capability to monitor, report, send alerts, and enable automated response to access management exceptions and violations.	N	
R1297.	2.27. Provide the capability to integrate and/or correlate threat intelligence and security information event management (SIEM) data with account activity.	N	
R1298.	2.28. Provide capability for account management for all platforms (e.g., Windows, Unix, Linux, Network, Network Devices, Managed Devices, Mac, Mainframe).	N	
R1299.	2.29. Provide the capability to document all role changes, template changes, and approval authorities in the identified secure online change management database.	N	
R1300.	2.30. Provide access to a self-service portal to provision, reactivate, modify, de-provision, suspend, and govern User accounts.	N	
R1301.	2.31. Provide an on demand ability to review access rights that have been granted.	N	
R1302.	2.32. Provide monitoring, reporting, alerting, and automated response to access management exceptions and violations as directed by Customer.	N	
R1303.	3. Support the Service Desk performing the following tasks:	N	
R1304.	3.1. Provide each Customer with the capability to exercise its authority for approval of all physical access and data and System access requests.	N	
R1305.	3.2. Notify the Customer regarding the entities and personnel to be granted access to Supplier-operated Systems and the level of Security access granted to each.	N	
R1306.	3.3. Follow Customer's instructions and procedures regarding such access as designated by Customers	N	
R1307.	3.4. Provide for policies and processes that prefer a least-privilege approach to granting access.	N	

Ref#		Requirement	Comply (Y/N)	Supplier Response
R1308.	3.5.	Provision, reactivate, de-provision, suspend, and govern accounts as directed by Customer.	N	
R1309.	3.6.	Mass provision, reactivate, de-provision, suspend, and govern accounts as directed by Customer.	N	
R1310.	3.7.	Temporary account provisioning, reactivation, de-provisioning, suspension, and governance as directed by the Customer.	N	
R1311.	3.8.	Support and enable processes for the delegation of provisioning, reactivation, de-provisioning, suspension, and governance of accounts for individual agencies while maintaining centralized governance with VITA.	N	
R1312.	3.9.	Provide Customers with the capability to exercise authority for approval of all data and System access requirements.	N	
R1313.	3.10.	Provision, reactivate, de-provision, suspend, and govern accounts utilizing federated identities, supporting all Federal Assurance Levels (FAL), as defined in NIST 800-63 and the Service Management Manual.	N	
R1314.	3.11.	Provision, reactivate, de-provision, suspend, and govern single sign-on capability for all accounts requiring this functionality as directed by Customers.	N	
R1315.	3.12.	Provision, reactivate, de-provision, suspend, and govern multi-factor authentication (MFA) capability for all accounts requiring this functionality as directed by Customers	N	
R1316.	3.13.	Perform on-demand access audits at the request of the Customer.	N	
R1317.	3.14.	Create and modify custom workflows as directed by Customer.	N	
R1318.	3.15.	Maintain and provide access to IAM reporting dashboard with multiple tiers of reporting and management access as directed by Customer.	N	
R1319.	3.16.	Manage log retention as directed.	N	
R1320.	3.17.	Provide for and manage password vault deployment and support as directed by Customer.	N	
R1321.	3.18.	Follow the Customer’s instructions and procedures regarding such access as designated by Customer	N	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1322.	4. Provide ability for Customer to grant role-based permissions.	N	
R1323.	5. Notify the Customers regarding the entities and personnel to be granted access and the level of access granted to each.	N	
R1324.	6. Follow Customer's instructions and procedures regarding such access as designated by Customers.	N	
R1325.	7. Maintain Security rules and access rights according to Customer's notifications and revise from time to time regarding these rights and rules.	N	
R1326.	8. Provide for policies and processes that prefer a least-privilege approach to granting access.	N	
R1327.	9. Conduct a review of access that has been granted with VITA and Customers at least on a quarterly basis.	N	
R1328.	10. Monitor, report and address access management exceptions and violations.	N	
R1329.	11. Establish procedures, forms, and approval levels for assigning, resetting, and disabling access by designated users, subject to Customer's review.	N	
R1330.	12. Implement and maintain a secure online database of all requests for access, access rights granted, and access approval authorities.	N	
R1331.	13. Ensure that access privileges for Supplier and Service Tower Supplier personnel are promptly removed upon departure from the ITISP.	N	
R1332.	14. VITA will have the ability to authorize Customers to grant or remove access privileges as required for onboarding, off-boarding, and emergency off-boarding.	N	
R1333.	15. Customers will have access to view and change access privileges only for their own data and systems.	N	
R1334.	**3.5.7.1 Physical Access Management**		
R1335.	*Supplier's responsibilities include:*		
R1336.	1. Provide Customers with the capability to manage access as granted to all the Supplier and Service Tower Supplier for all VITA and Customer facilities.	Y	
R1337.	2. Implement VITA security standards, guidelines, and procedures regarding access control and facility hardening measures to prevent unauthorized access or damage to facilities that contain VITA data and information processing systems and equipment.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1338.	**3.5.7.2 Logical Access Management**		
R1339.	*Supplier's responsibilities include:*		
R1340.	1. Provide Customers with the capability to manage and administer access to all the Supplier and Service Tower Supplier operated Systems, Networks, Software, and Customers data.	Y	
R1341.	2. Implement a process that enables Customer's IT Security department to exercise full administrative rights to the Systems providing the Services, including full access to audit trails and logs.	Y	
R1342.	3. Establish processes and controls for administrating IDs and passwords used for data or System, including:	Y	
R1343.	3.1. Executing all related administration for user identification (IDs) and passwords.	Y	
R1344.	3.2. Administering user IDs and passwords for Service Tower Supplier operated Systems.	Y	
R1345.	**3.6 Data Security**		
R1346.	**3.6.1 Managed Encryption** **Managed Encryption Platform suspended on April 1, 2022**		
R1347.	*Data security includes security controls that are intended to protect Commonwealth data. Data may traverse or be stored both within and outside the Managed Environment. The controls included in this section focus on protecting the data itself with controls such as encryption. Supplier will provide a multi-tenant encryption management suite that meets or exceeds the requirements set forth by VITA and its Customers.* *Supplier's responsibilities include:*		Suspended on April 1, 2022
R1348.	1. All Systems that Handle Confidential Information will encrypt Commonwealth data including Confidential Information in transit using algorithms and key lengths consistent with the most recent VITA Rules and as specified in the Service Management Manual.	Y	Suspended on April 1, 2022
R1349.	2. Utilize the encryption protocol as specified in the Service Management Manual with 128-bit or larger key size.	Y	Suspended on April 1, 2022

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1350.	3. Utilize a Third Party provider approved by VITA and the Customer that is a recognized and trusted authority in the industry to generate any certificates that are used for authentication.	Y	Suspended on April 1, 2022
R1351.	4. Web Applications containing Confidential Information will be transmitted over encrypted channels. Attempts to use the Application without encryption will be rejected.	Y	Suspended on April 1, 2022
R1352.	5. Confidential Data at rest will be protected by encryption as defined in the Service Management Manual.	Y	Suspended on April 1, 2022
R1353.	6. Keep private keys confidential, implement key lifecycle management and protect all keys in storage or in transit.	Y	Suspended on April 1, 2022
R1354.	7. Choose keys randomly from the entire key space and ensure that encryption keys allow for retrieval for administrative and/or forensic use.	Y	Suspended on April 1, 2022
R1355.	8. VITA and the Customer will receive a complete set of decryption keys. All Commonwealth data will be recoverable.	Y	Suspended on April 1, 2022
R1356.	9. VITA requires that the use, storage, and/or handling of Commonwealth Data occur within the contiguous United States.	Y	Suspended on April 1, 2022
R1357.	10. The Commonwealth will maintain control of the encryption keys that allow access to Commonwealth data, unless otherwise specified in the Service Management Manual.	Y	Suspended on April 1, 2022
R1358.	11. Provide a multi-tenant solution based on industry standard encryption standards that supports:		Suspended on April 1, 2022
R1359.	11.1. Handling keys from every major encryption algorithm, plus all the communications and exchange standards (and proprietary methods) to manage keys inside and outside the system or service location where they are stored.	Y	Suspended on April 1, 2022
R1360.	11.2. Entitlement decisions that are derived from the identities of the entities involved. Keys will have identifiable owners (binding keys to identities).	Y	Suspended on April 1, 2022
R1361.	11.3. Lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions.	Y	Suspended on April 1, 2022

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1362.	11.4. Strong encryption (e.g., AES-256) in open/validated formats and standard algorithms. Keys will be maintained in dedicated a Hardware Security Module (HSM) by VITA, the Supplier or trusted key management provider under management of the Supplier.	Y	Suspended on April 1, 2022
R1363.	11.5. The provided platform will be hardened to the extent needed for VITA Rules compliance.	Y	Suspended on April 1, 2022
R1364.	11.6. Support for key communications standards and platforms to exchange keys, which may include a mix of proprietary implementations (e.g., a specific database platform) and open standards (e.g., the evolving Key Management Interoperability Protocol [KMIP]).	Y	Suspended on April 1, 2022
R1365.	11.7. Support for rotating keys in common applications.	Y	Suspended on April 1, 2022
R1366.	11.8. Hierarchical key deployment support to create a “manager of managers” to enforce consistent policies across individual-system boundaries and throughout distributed environments.	Y	Suspended on April 1, 2022
R1367.	11.9. Keys should be accessible by the designated users within the data owning Customer.	Y	Suspended on April 1, 2022
R1368.	11.10. Keys should be available for individual applications and accessible by designated user(s).	Y	Suspended on April 1, 2022
R1369.	11.11. Backup and restoration should be achieved in a secure manner.	Y	Suspended on April 1, 2022
R1370.	12. Provide role-based access to all tenants that supports:		Suspended on April 1, 2022
R1371.	12.1. A system-admin role for administration of the key manager itself, with no access to the actual keys.	Y	Suspended on April 1, 2022
R1372.	12.2. Limited administrator roles that allow access to subsets of administrative functions such as backup and restore, creating new key groups, etc.	Y	Suspended on April 1, 2022
R1373.	12.3. An audit and reporting role for viewing reports and audit logs with granularity of access to certain audit logs (e.g., specific applications).	Y	Suspended on April 1, 2022
R1374.	12.4. System/application manager roles for individual system and application administrators who need to generate and manage keys for their respective responsibilities.	Y	Suspended on April 1, 2022

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1375.	12.5. Sub-application manager roles which only have access to a subset of the rights of a system or application manager (e.g., create new keys only but not view keys).	Y	Suspended on April 1, 2022
R1376.	12.6. System/application roles for the actual technical components that need access to keys.	Y	Suspended on April 1, 2022
R1377.	13. Auditing		Suspended on April 1, 2022
R1378.	13.1. Type of activity to audit include:		Suspended on April 1, 2022
R1379.	13.1.1. All access to keys	Y	Suspended on April 1, 2022
R1380.	13.1.2. All administrative functions of the key manager	Y	Suspended on April 1, 2022
R1381.	13.1.3. All key operations – including generating and rotating keys	Y	Suspended on April 1, 2022
R1382.	13.2. Support for logging of all activity to a centralized log management solution.	Y	Suspended on April 1, 2022
R1383.	13.3. Support for the real-time exporting of raw audit logging information to customer maintained systems.	Y	Suspended on April 1, 2022
R1384.	14. Provide security controls over the encryption key management process:		Suspended on April 1, 2022
R1385.	14.1. A policy enforcement framework for controlling workflow processes as well as for controlling attributes such as key lengths, validity periods, and cryptographic hash types	Y	Suspended on April 1, 2022
R1386.	14.2. Process to quickly identifying the misuse of keys	Y	Suspended on April 1, 2022
R1387.	14.3. Controls that prevent key-based outages	Y	Suspended on April 1, 2022
R1388.	14.4. Automated key replacement process for fast remediation if needed	Y	Suspended on April 1, 2022
R1389.	14.5. Full support for key archiving and recovery	Y	Suspended on April 1, 2022
R1390.	**3.6.2 eDiscovery / Preservation**		
R1391.	*This section identifies requirements for the solution the Supplier will provide, collecting and producing electronically stored information (ESI) in response to a request for production in a law suit or investigation. ESI includes emails, documents, presentations, databases, voicemail, audio and video files, and social media.* *To facilitate eDiscovery, the Supplier shall provide a solution that includes the following capabilities:*		Updated pricing for optional service forthcoming

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1392.	1. Log and archive all real-time communications including Email, Email attachments, Instant Messaging, Social Media, voice mail, and associated metadata in a centralized, tamper-proof environment.	Y	
R1393.	2. Search and discover all supported document types as described in the Managed Services Manual (for example, MS Office, Adobe, HTML, zip files, etc.)	Y	
R1394.	3. Retrieval of stored information based on granular searches of keywords, users, time frames, and complex Boolean searches.	Y	
R1395.	4. Supports searching on content containing international languages (Unicode).	Y	
R1396.	5. Search across all storage locations (desktop, network, cloud, etc.)	Y	
R1397.	6. Anti-tampering checksums for non-repudiation.	Y	
R1398.	7. Full binary capture.	Y	
R1399.	8. Integration with VITA email system.	Y	
R1400.	9. Implementing litigation holds/preservation orders in a multi-tenant environment that includes all platforms, file types, and storage locations.	Y	
R1401.	10. Scan and identify viruses or Malware embedded in ESI.	Y	
R1402.	11. Accounts for name changes, aliases, and different naming conventions that may relate to the custodians being searched.	Y	
R1403.	12. Support for collection of multiple searches to place records into a legally defensible, secured location for each legal matter.	Y	
R1404.	13. Capable to scan encrypted storage media.	Y	
R1405.	**3.6.3 Certificate/Key Management**		
R1406.	*Supplier will provide a multi-tenant management suite for certificate management, secure key storage, and secure access to digital certificate management services.* *Supplier's responsibilities include:*		

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1407.	1. Provide a multi-tenant solution based on industry standard encryption standards that supports:	Y	
R1408.e	1.1. Open Standards based with broad support for tokens and smart cards	Y	
R1409.	1.2. Standards-based PKI security for user authentication and electronic signatures.	Y	
R1410.	1.3. Support for strong ECC (Elliptic Curve Cryptography)	Y	
R1411.	1.4. Support for both soft and a wide assortment of physical tokens	Y	
R1412.	2. Provide keys and certificates for browsers, Web servers, smart cards, network devices, etc.	Y	
R1413.	3. Complete electronic ID production process, from key generation and smart card profiling to the distribution of PIN codes to the end user.	Y	
R1414.	4. Integration with National Digital IDs or private Certificate Management of any required level of assurance (LoA).	Y	
R1415.	5. Provide the following capabilities for issuance and tracking of certificates:	Y	
R1416.	5.1. Non-intrusive management for the end users	Y	
R1417.	5.2. Automated issuance and renewal process	Y	
R1418.	5.3. Delegated/self-service credential management; supports multi-tenancy; through a web-based, self-service portal for certificate requests and renewals	Y	
R1419.	6. Provide security controls over the certificate management process:	Y	
R1420.	6.1. A policy enforcement framework for controlling workflow processes as well as for controlling attributes such as key lengths, validity periods, and cryptographic hash types	Y	.
R1421.	6.2. Process to quickly identifying the misuse of keys and certificates	Y	
R1422.	6.3. Controls that prevent certificate-based outages	Y	
R1423.	6.4. Automated key and certificate replacement process for fast remediation if needed	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1424.	6.5. Support standard protocols and provide unique solutions for integration with current IAM (Identity and Access Management) systems through SAML integration	Y	
R1425.	6.6. Full support for key archiving and recovery	Y	
R1426.	6.7. Ensure keys protecting Commonwealth data remain in control of the Commonwealth	Y	
R1427.	**3.6.4 Tokenization – Deleted**		
R1428.			
R1429.	~~1.~~		
R1430.	~~2.~~		
R1431.	~~3.~~		
R1432.	~~4.~~		
R1433.	~~5.~~		
R1434.	~~6.~~		
R1435.	~~7.~~		
R1436.	~~8.~~		
R1437.	~~9.~~		
R1438.	~~10.~~		
R1439.	~~11.~~		
R1440.	~~12.~~		
R1441.	**3.6.5 Data Loss Prevention**		

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1442.	*The Supplier will provide a centrally managed, multi-tenant data loss prevention (DLP) solution to the Customer that will help mitigate the loss or breach of sensitive data as defined by the Customer.*		
R1443.	1. Solution will discover, classify, monitor, and protect Customer data whether on premise or in hosted environment.	Y	
R1444.	2. Solution will be capable of scanning all data stores, including databases, file shares, electronic mail, local workstations, cloud storage, mobile devices, etc. and discovering sensitive data, including social security numbers, credit card numbers, financial information, and intellectual property.	Y	
R1445.	2.1. Solution will scan structured and unstructured data.	Y	
R1446.	2.2. Solution will watermark/fingerprint unstructured data for detection.	Y	
R1447.	2.3. Solution will offer exact data matching, pattern matching, regex, etc.	Y	
R1448.	2.4. Solution will scan across all platforms and all file formats including but not limited to .doc, .xls, .pdf, source code, text files, images, custom files, etc.	Y	
R1449.	3. The Customer will be able to customize scan, data loss, and remediation policies based on business needs and in compliance with “VITA Rules”.	Y	
R1450.	4. Solution will provide the Customer the capability to apply remediation policies based on the classification and sensitivity of the data discovered. The Customer will be able to tag, quarantine, block, or delete sensitive data as it is discovered.	Y	
R1451.	5. The Supplier will provide discovery scanning via agent and agentless methods.	Y	
R1452.	6. The Supplier will provide a dashboard to Customers that will provide an overview of discovery scans in accordance with Service Management Manual.	Y	
R1453.	7. Solution will scan data via encrypted and unencrypted communication channels.	Y	
R1454.	8. Solution will provide a central DLP platform that integrates with all services provided by Suppliers transmitting or storing Commonwealth data.	Y	
R1455.	9. Solution will support multi-factor authentication via directory services and integrate with the existing IAM solution.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1456.	**3.6.6 Data Removal / device disposal**		
R1457.	*The Supplier will provide a solution, at a minimum, that adheres to the Commonwealth security standards, VITA Rules, and include the following approaches for data sanitization (this includes data stored on Supplier devices):*		
R1458.	1. All data removal and sanitization will occur in accordance with VITA Rules and the Service Management Manual.	Y	
R1459.	2. The data removal and sanitization process will be subject to audit and in-person review.	Y	
R1460.	3. Documentation for data removal and sanitization will be submitted to identified parties as described in the Service Management Manual.	Y	
R1461.	4. Commonwealth data will be removed and sanitized from any system containing the data, this includes wiping of virtual systems.	Y	
R1462.	**3.6.7 Enterprise Remote Access**		
R1463.	Implement Site-to-Site VPN connections for all VITA-approved Third-Party sites for agency connectivity and other VITA Suppliers and designated Third Party Vendors as required	Y	
R1464.	Maintain Site-to-Site VPN Networking environment as required to meet VITA and VITA Customer business and Application requirements.	Y	
R1465.	Provide method for VITA and VITA Customers to utilize secure tunnels across the Internet to connect to the Commonwealth Network using Network Access tools	Y	
R1466.	Configure Intrusion Detection and Intrusion Prevention technologies into the solution.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1467.	Support the capability to dynamically create and discontinue split tunnels persistence based on traffic patterns and Customer requirements.	Y	
R1468.	Configure and maintain mechanisms to meet multiple agency security and application requirements for remote access.	Y	
R1469.	Partition the Remote User Access based on User ID such that multiple Customers can securely share the Remote User Access solution. Including Support for multiple organizations and sub-organization relationships. Support customer defined access control policies and support policy enforcement of access authority.	Y	
R1470.	Provide reporting capabilities available within the system to meet Customer audit and compliance requirements.	Y	
R1471.	Provide the capability for the use of the Remote User Access by Third Party Vendors with User ID who provide support for Data Center services via an Internet connection.	Y	
R1472.	Provide a feed for audit data to the Commonwealth SIEM and the MSI per the SMM.	Y	
R1473.	Supplier shall provide connectivity through secure VPNs between VITA Sites, as designated by VITA.	Y	
R1474.	Provide for secure, reliable and highly available remote access connectivity between customer sites and VITA enterprise Data Center.	Y	
R1475.	Implement Customer-specified access control policies.	Y	
R1476.	Implement policy enforcement of access authority.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1477.	Act as a single point of contact for the management of the Remote User Access.	Y	
R1478.	Provide mechanisms to meet multiple agency security and application requirements for remote access	Y	
R1479.	Secure remote access via a secure channel (VPN), using strong cryptography and Security protocols (e.g. SSL/TLS, IPSEC, SSH) to safeguard sensitive data during transmission over public Networks.	Y	
R1480.	Provide for secure, reliable and highly available remote access connectivity into Data Center core Networks from other Networks, VITA Customer Networks, the public Internet and other industry standards-based Third Party Vendor Networks.	Y	
R1481.	Authorize and restrict access based on multiple factors (e.g. agency, security group, User name)	Y	
R1482.	Incorporate two-factor authentication for remote access (Network-level access originating from outside the Network) to the Network.	Y	
R1483.	Support single-factor and multi-factor authentication mechanisms via Prisma.	Y	
R1484.	Provide, support, and manage remote access Software clients for client-to-Site usage	Y	
R1485.	Provide secure remote access, including clientless access to authorized web Applications, client/server Applications, voice, and file sharing to VITA and VITA Customers, and designated Third Party Vendors	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1486.	Enable secure access from public End-User Computing devices	Y	
R1487.	Implement Site-to-Site VPN connections for VITA-approved Agency sites to provide secure connectivity in support of the Enterprise SD-WAN service	Y	
R1488.	**3.6.8 Cloud Access Security Broker (CASB)**		
R1489.	Atos will provide the day-to-day monitoring and analysis as well as administrative services. The steady-state operations stage consists of the following discrete activities: • Platform support • Shadow IT services • Sanctioned IT services • IaaS Cloud Security Posture reporting • Execute security operations		
R1490.	**Steady State Platform Support**		
R1491.	Ensure stable integration with Cloud Service Providers (e.g. Box, Azure)	Y	
R1492.	Ensure stable integration with on-prem components (MDM, SIEM,LDAP, etc.)	Y	
R1493.	Ensure integration with Cloud components (e.g. SSO)	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1494.	Ensure the Enterprise Connector(s) are operationally sound andworking	Y	
R1495.	**Shadow IT Services**		
R1496.	Monitor Shadow IT activity	Y	
R1497.	Manage Shadow IT governance (service groups, watchlists, etc.)	Y	
R1498.	Shadow IT Forensic Analysis	Y	
R1499.	Manage Service Requests	Y	
R1500.	Implementation of Shadow IT enforcement policies	Y	
R1501.	**Sanctioned IT services (SaaS)**		
R1502.	Monitor Sanctioned IT activity	Y	
R1503.	Monitor and respond to threat protection alerts.	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1504.	Monitor and respond to policy related incidents.	Y	
R1505.	Fine-tune policies (Anomaly Settings, Access control, DLP)	Y	
R1506.	General Administration (restore quarantined documents, approve access control requests, create new reports, etc.)	Y	
R1507.	**Cloud Infrastructure monitoring services (IaaS)**		
R1508.	Monitor IaaS activity	Y	
R1509.	Monitor and respond to threat protection alerts.	Y	
R1510.	Monitor and respond to policy related incidents.	Y	
R1511.	Fine-tune policies (Anomaly Settings, Access control, DLP)	Y	
R1512.	Monitoring and Report Security Posture of IaaS Services	Y	
R1513.	General Administration (restore quarantined documents, approve accesscontrol requests, create new reports, etc.)	Y	

Ref#	Requirement	Comply (Y/N)	Supplier Response
R1514.	**Execute Security Operations**		
R1515.	Event monitoring Review system status	Y	
R1516.	Incident management • Open Incident cases • Execute current practices and procedures	Y	
R1517.	Reporting • Generate reports • Demonstrate scheduled report tasks	Y	
R1518.	Problem management • Problem detection • Escalation path	Y	