PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS (VA)
Information Technology (IT) Field Security Operations
Critical Infrastructure Protection Service

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOLUTION

Date: May 28, 2014
TAC-14-13183
PWS Version Number: 1.8

Contents

Security Information and Event Management (SIEM) Solution
TAC Number: TAC-14-13183

1.0 BACKGROUND

The Department of Veterans Affairs (VA) Network and Security Operations Center (NSOC) provides network and security incident management capability for the VA Enterprise. The 24x7x365 operations center has two locations in facilities at Hines, IL and Martinsburg, WV. The NSOC monitors overall health of the network in addition to performing the full range of functions across the spectrum of activities relating to incident management and response, and monitors the cyber security posture of the Department across the Continental United States (CONUS), Philippines, and Europe. The infrastructure consists of Intrusion Prevention System (IPS) devices; host servers; desktops/laptops; and routers and switches (reference Section 5.3 for specific quantities). The VA also utilizes other network devices and tools such as: firewalls (currently F5 and Palo Alto), Domain Name System (DNS) Blackhole, Access Control Servers, Domain Name System Security Extensions (DNSSEC), Email Security Appliances (currently IronPort), Antimalware for web threats (currently WebWasher), Internet Cache (currently NetCache), Network Intrusion Prevention and Detection systems, Anti-Virus, Host Based Intrusion Prevention Systems, Network Discovery, Compliance Scanning, Vulnerability Scanning and Security Management servers (currently ePolicy Orchestrator (ePO)) to secure the VA network. These network devices and tools monitor the overall health of the network using a variety of management systems in a distributed architecture that is centrally monitored and managed from NSOC organizational units in Martinsburg, WV and Hines, IL.

As mandated in OMB memorandum M-14-03 and Federal Trusted Internet Connections (TIC) manadates, the NSOC is charged with the requirement to manage information security risk on a continuous basis which includes the requirement to monitor the security controls in Federal information systems and the environments in which those systems operate on an ongoing basis. In order to accomplish this task a Security Information Event Management solution is required.

The VA NSOC serves as VA's security operation element under the Office of Information Security (OIS). In order to mitigate recent audit material weaknesses, implement continuous monitoring as outlined in OMB M-14-03 and enhance the security of Veterans' data, the NSOC will also install a solution with associated hardware to support the VA.

The proposed SIEM solution will support NSOC's mandate to manage, protect and monitor the cyber security posture of the entire VA Enterprise. This SIEM will augment NSOC's ability to perform analyses of cyber security events; maintain detailed logs and databases of VA cyber security incidents and responses; and generally perform the full range of functions across the spectrum of activities relating to incident management and response, vulnerability scanning, event correlation and analysis, audit log analysis, patch distribution and remediation planning.

2.0 APPLICABLE DOCUMENTS

Documents referenced or germane to this Performance Work Statement (PWS) are listed below. In the performance of the tasks associated with this PWS, the Contractor shall comply with the following:

1. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002"
2. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
3. FIPS Pub 201, "Personal Identity Verification of Federal Employees and Contractors," March 2006
4. 10 U.S.C. § 2224, "Defense Information Assurance Program"
5. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
6. 42 U.S.C. § 2000d **"**Title VI of the Civil Rights Act of 1964"
7. Department of Veterans Affairs (VA) Directive 0710, "Personnel Suitability and Security Program," September 10, 2004
8. VA Directive 6102, "Internet/Intranet Services," July 15, 2008
9. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
10. OMB Circular A-130, "Management of Federal Information Resources," November 28, 2000
11. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
12. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, March 2005
13. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
14. Homeland Security Presidential Directive (12) (HSPD-12)
15. VA Directive 6500, "Information Security Program," August 4, 2006
16. VA Handbook 6500, "Information Security Program," September 18, 2007
17. VA Handbook, 6500.5, Incorporating Security and Privacy in System Development Lifecycle
18. VA Handbook 6500.6, "Contract Security," March 12, 2010
19. Program Management Accountability System (PMAS) portal (reference PWS References -Technical Library at https://www.voa.va.gov/)
20. OED ProPath Process Methodology (reference PWS References -Technical Library and ProPath Library links at https://www.voa.va.gov/) NOTE: In the event of a conflict, OED ProPath takes precedence over other processes or methodologies
21. Technical Reference Model (TRM) (reference at http://www.ea.oit.va.gov/Technology.asp)
22. National Institute Standards and Technology (NIST) Special Publications
23. VA Project Management Guide (available upon request)
24. OMB Memorandum, "Transition to IPv6", September 28, 2010

25. The Office of Management and Budget (OMB) Circular A-130, Appendix III; Security of Federal Information Resources
26. National Institute of Standards and Technology (NIST) Special Publication, (SP) SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations
27. National Institute of Standards and Technology (NIST) Special Publication, (SP) SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations
28. "Enhancing the Security of Federal Information and Information Systems", OMB Memorandum M-14-03, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf

3.0 SCOPE OF WORK

The Contractor shall provide two (2) independent SIEM systems that include hardware, software and licensure to collect and manage security information event data. "System" is defined here as the working solution that includes all elements integrating together to satisfy the requirements herein. The systems shall leverage and be fully compatible with VA's existing Splunk[1], as described herein. One system (Production system) shall reside in the production TIC environment. The second system (Test system) shall reside in the Test lab. The Contractor shall provide installation, training, professional engineering services, testing, Accreditation & Authorization (A&A) documentation support and product support services.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance shall be one 12-month base period with two 12-month option periods. This will be a firm fixed price delivery order. If performance is required at a Government facility, then the Contractor shall comply with the following holidays.

There are ten (10) Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

Under current definitions, four are set by date:

New Year's Day	January 1
Independence Day	July 4
Veterans Day	November 11
Christmas Day	December 25

If any of the above falls on a Saturday, then Friday shall be observed as a holiday. Similarly, if one falls on a Sunday, then Monday shall be observed as a holiday.

[1] Splunk is an operational intelligence platform that collects and indexes any machine data from virtually any source in real time. Splunk also performs search, monitor, analyze and visualize your data to gain new insights and intelligence.

The other six are set by a day of the week and month:

Martin Luther King's Birthday	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Thanksgiving	Fourth Thursday in November

4.2 PLACE OF PERFORMANCE

Tasks under this PWS shall be performed in Contractor facilities and VA facilities as listed in the table in Section 5.9.

4.3 TRAVEL

The Government anticipates travel under this effort to perform the tasks associated with the effort, as well as to attend program-related meetings or conferences through the period of performance. Include all estimated travel costs in your firm-fixed price line items. These costs will not be directly reimbursed by the Government.

The total estimated number of trips in support of the program related meetings for this effort is one. The Contractor is required to travel to Martinsburg, WV at the VA Capital Region Readiness Center (CRRC) to attend the kick-off meeting.

Purpose/Location	# of Trips	Duration of Each Meeting	# of Attendees
Kick-off Meeting – CRRC	1	3 days	3

The estimated number of days for meetings identified in the preceding table does not include Contractor travel time.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.1 PROJECT MANAGER

The Contractor shall provide a Project Manager (PM) to ensure the success of the project. The Contractor PM shall support the VA PM with communications of project activities, manage risk, cost, and schedule. The Contractor shall propose Project Management in accordance with solution provided (i. e. if Splunk is the presented solution, PM services are reduced as training, implementation and engineering services are reduced as described herein).
Project management tasks shall include the following:

A. Communicate on a weekly basis to provide project status updates to VA PM;

B. Provide day-to-day project management guidance and direction for their project team members in the execution of tasks defined in this PWS;

C. Capture technical and lessons learned information from the project team members and synthesize into actionable information to be used by VA Project team;

D. Monitor compliance with contract requirements and address any scope changes that might impact cost, schedule, quality or external dependencies as well as any schedule variances;

E. Facilitate and coordinate required project meetings (i.e., Kick-off meeting, weekly telephonic Project Status Meetings) and follow-on activities. Tasks shall include coordinating meetings, developing agendas, documenting meeting minutes and action items, and providing recommendations;

F. Ensure Contractor personnel performing onsite activities have properly coordinated well in advance with each facility; and

G. Review all required deliverables within this PWS for accuracy and ensure on-time delivery.

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall provide a detailed Contractor Project Management Plan that is responsive to this PWS and describes in further detail the approach to be used for each aspect of the task order as defined in the technical proposal based on the VA Project Management Guide, available from the VA Internet at: https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=27.

The purpose of this plan is to ensure that, at a minimum, the Contractor understands and manages risk, communications, finances, schedules, quality and human resources. The plan shall include the following:

5.1.1.1 Project Scope Plan shall document how the project scope will be defined, managed, controlled, verified and communicated to the Contractor's and the Government's project team.

5.1.1.2 Schedule Management Plan shall include a schedule of deliverables. The schedule shall define the approach the Contractor shall use to create, monitor and control the project schedule, to include deliverable dependencies and interdependencies,and how changes will be managed once the schedule is approved.

5.1.1.3 Communication Management Plan identifies the formal communication methodology for the project.

5.1.1.4 Risk Management Plan the Contractor shall document foreseeable risks and a response plan to mitigate those risks.

5.1.2 PROJECT RELATED MEETINGS

The Contractor shall support weekly Project Status Meetings via teleconference from the inception of the Contract throughout the period of performance. The Contractor shall be prepared to discuss any concerns and issues identified in each Bi-Weekly

Status Report (BWAR). At the conclusion of each meeting, the Contractor shall prepare the minutes summarizing the discussion items.

Deliverables:

A. Contractor Project Management Plan
B. Project Scope Plan
C. Schedule Management Plan
D. Communication Management Plan
E. Risk Management Plan

5.2 KICKOFF MEETING AND BIWEEKLY REPORTING

5.2.1 KICKOFF MEETING

The Contractor shall not commence performance on the tasks required by this PWS until the Contracting Officer (CO) or Contracting Officer's Representative (COR) has conducted the Kick-off Meeting. At this Kick-off Meeting, the Contractor shall give a presentation, utilizing Microsoft PowerPoint, explaining how the Contractor will accomplish the objectives of the Task Order. The Contractor's key personnel shall brief for their respective project areas. The Kick-off Meeting should be held within five days after award. The meeting will be held in Martinsburg, WV. The Contractor shall provide "Soft" (electronic) copies in advance of the briefing, specific email addresses to be provided by the COR at least one day in advance of the Kick-off Meeting. At the conclusion of the meeting, the Contractor shall prepare the minutes of the meeting and distribute them to the CO, VA PM and COR. The requirement for a Kick-off Meeting may not waive any formal post-award requirement as determined by the CO.

5.2.2 REPORTING REQUIREMENTS

The Contractor shall provide Bi-Weekly Activity Reports (BWAR) that will identify all issues, prospective scope changes, and progress to date against project milestones over the last reporting period and expected results for the next reporting period.

The BWAR shall cover all work completed during the reporting period and work planned for the subsequent reporting period. Each report shall also identify any problems that arose and a description of how the problems were resolved. If problems have not been completely resolved, then the Contractor shall provide an explanation and plan for corrective action. The Contractor shall be prepared to discuss the report with the VA CO, COR and PM. The Contractor shall monitor performance against the CPMP and report any deviations. It is expected that the Contractor will keep in communication with the VA Contracting Officer, VA PM, and COR accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues. The Contractor is responsible for providing written notice to the Contracting Officer, VA PM and COR for issues at risk of impacting overall schedule completion. The Contractor shall provide the VA CO, VA PM, and COR with BWARs in electronic form in Microsoft Word (.doc)

and Project (.mpp) formats. Each report shall reflect data as of the last day of the preceding week.

Deliverables:

A. Kick-off Meeting Presentation
B. Bi-Weekly Activity Report

5.3 GENERAL REQUIREMENTS

The Contractor shall provide a turn-key solution that includes: hardware, software, third party software, and licensure to collect and manage security information event data. The system shall integrate with and be fully compatible with the VA's existing Splunk. The system shall reside in the production environment with sensors and management software instances, to include four Trusted Internet Connection (TIC) Gateways.

The Contractor shall deploy the architecture for the primary NSOC locations. (See Attachment 1 which will depict TIC gateways). The Contractor shall provide systems that provide High Availability (HA) at each location. HA is defined here to mean a system with an immediate in-place back up, and work in an active-active mode.

An additional system shall be provided that will reside in the test lab in Martinsburg, WV and be configured to replicate a SIEM system in the TIC Gateway production environment (the Lab will replicate only one TIC gateway). This shall include the same device types, model(s), and mirror the HA configuration implemented in the TIC Gateway production environment. The test lab is isolated from, and has no connectivity to, the production environment.

The proposed production systems shall provide 24x7x365 collection and management of security information event data.

The proposed production system shall have HA; and work in an active-active mode. Active-Active is defined as both are always working; one is not on standby waiting for the other to fail. Preventing loss of data is critical.

The Contractor shall provide product details to include:

a. Estimated bandwidth based on proposed architecture
b. Storage volume based on proposed architecture
c. Hardware specifications
d. Licensing model

Deliverables:

A. SIEM Hardware
B. SIEM Software

5.4 SIEM SOLUTION REQUIREMENT

The Contractor shall provide a turn-key SIEM Solution to include hardware, software (including any third party software), installation, software license, software configuration documentation, training, implementation services, testing and software/hardware maintenance to be implemented at each VA NSOC site to meet the requirements identified in this PWS.

5.4.1 System Requirements

The SIEM Solution shall satisfy all of the following requirements:

SIEM SOLUTION REQUIREMENT

Requirements	Met Yes/ No
1. Platform Requirements	
1.1. Shall address all major SIEM use cases including:	
1.1.1. Seamless integration with Splunk	
1.1.2. Incident investigations and workflow	
1.1.3. Forensics support	
1.1.4. Security and compliance reporting and visualizations	
1.1.5. Real time monitoring and alerting on both known and unknown threats	
1.1.6. Shall do cross-data source correlations to detect specific patterns	
1.1.7. Full text search of all ingested data using pattern matching and regular expressions	
1.1.8. Long-term data retention	
1.2. Single, integrated product for both logging and SIEM use cases (no separate logging and SIEM data stores/UIs)	
1.2.1. Shall integrate seamlessly with Splunk for Log management and Long-term data retention	
1.2.2. Single user interface for all system functionality including searching, reporting, rule building, and system administration.	

1.2.3. Single, common data store for all indexed data	
1.2.4. Single search or report can encompass all the indexed data	
2. Data Requirements	
2.1. Scalable architecture capable of supporting customer deployments with the following parameters:	
2.1.1. Shall be able to index a minimum of 4TB of incoming log data per day, with scalability up to 32TB per day	
2.1.2. Shall be able to ingest maximum rates of up to 200 GB per hour of incoming log data, with scalability to handle maximum rates of up to 2.5TB per hour.	
2.1.3. Shall be able to scale horizontally	
2.1.4. Data must be searchable immediately after indexing	
2.1.5. Data collected shall be retained and stored local to each site	
2.1.6. Shall be able to correlate data from distributed collections points from a centralized manager	
2.2. Shall use a schema-less data store (not a relational database with fixed schema)	
2.3. Ability to index all the original, unmodified data and make it searchable and reportable (no data normalization or data loss)	
2.4. Shall scale out on hardware with no fixed limit on storage (add more hardware as needed)	
2.5. Shall automatically ingest different data types into different indices for optimal search performance or data segregation/RBAC purposes	
2.6. Shall handle timestamps from different time zones	
2.7. Automatic compression of indexed data to reduce storage requirements	
2.8. Shall include storage resources to support Splunk to	

the following levels:	
2.8.1. Storage resource for Splunk to handle 4TB of data per day for 365 days a year in searchable indices, with the ability to scale in excess of 32 TB per day	
2.8.2. Tier 1 Storage for online data must meet a minimum of 800 IOPS	
2.8.3. Requires a minimum of 500 TB of Tier 1 storage per site to allow for logging levels to fluctuate between sites	
2.8.4. Tier 2 storage resources to maintain 2 additional years of data available on-demand	
2.8.5. Resources to provide data backups for solution including Splunk, data backup solution cannot require hand-on maintenance	
2.8.6. Backup solution shall encompass full system backups, as well as data backups for all tier 1 and tier 2 storage	
2.8.7. Storage shall include a “non-returnable” disk clause in compliance with VA requirements	
2.9. Flexible data retention settings:	
2.9.1. Options to retain indexed data as long as desired (days, months, or years)	
2.9.2. Granular control on what happens to data as it ages	
2.9.3. Shall be able to support automatic, seamless archival of data into compressed and uncompressed formats on external/cost effective storage	
2.10. Ability for index replication to maintain multiple, identical copies of indexed data for data availability, data fidelity, disaster tolerance, and improved search performance	
2.11. Ability and sufficient storage resources for system settings, scheduled queries, scheduled reports, and all other configurations and settings to be replicated from	

the live system to the backup system regularly	
3. Infrastructure Requirements	
3.1. Shall be entirely virtualized with no requirement for specialized physical appliances	
3.1.1. All necessary operating system licensing, and virtualization hardware and licensing must be included.	
3.1.2. Perpetual software licenses that cover patches and version updates must be included	
3.2. Compatible with all major operating systems	
3.3. Implements a certified converged infrastructure	
3.3.1. Server, network and storage components completely integrated and operating on an overlying hypervisor	
3.3.2. Management seamlessly compatible with existing UCS infrastructure components and VMware hypervisor	
3.3.3. Advanced remote management for all components in the converged infrastructure shall be included	
3.3.4. All components of the converged infrastructure shall provide resiliency in case of component failure.	
3.4. Available footprint for solution is two 42U racks in each of the four TIC locations. If converged infrastructure components include racks, there shall be space for existing patch panel using 4U to be put in the top of the racks	
3.5. Computing resources to handle 1.5TB per day at each of 4 geographically dispersed sites	
3.6. Computing resources capable of handling up to 50 concurrent searches, in addition to SIEM analytic searching and processing requirements.	
3.7. Computing resources necessary for Splunk to be capable of searching 5TB of data in less than 5	

minutes.	
3.8. Computing resources shall include a minimum 400GB Memory and 250 CPU Cores per site	
3.9. End user access shall be through a browser-based UI that is compatible with all major browsers	
3.10. System requirements:	
3.10.1. The systems shall provide role-based access control (RBAC) to restrict access to views based on user's role.	
3.10.2. The systems shall create a detailed, non-modifiable log for operating system, application, administrator, and user activity to ensure proper accountability for the system.	
3.10.3. The systems shall store all passwords in an encrypted format and not display passwords on logon screens in clear text.	
3.10.4. The systems shall force users to logoff after a configurable period of time.	
3.10.5. The system shall include Active Directory Integration for account management and support PIV authenticated users with Windows pass-through authentication or similar.	
3.10.6. The systems shall provide security controls and audit ability as required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 and VA-Handbook 6500 for a high risk system.	
3.10.7. The systems shall provide an encrypted (TLS 2.0 or better) web accessible interface.	
3.10.8. The systems shall use https/ssl connections for any web-based access. The systems shall support customer provided SSL certificates, signed by an internal, customer hosted certificate authority. The solution shall support a private key with a minimum of 2048 bits.	
3.10.9. The systems' hardware shall be compatible with 110 volt power source and will	

include IEC C13 or NEMA 5 power cords compatible with specific power distribution unit (PDU) plug types specified for each location.	
3.10.10. The systems shall provide all network connectivity, including cabling and small form-factor pluggable (SFPs) if needed, to attach to existing 10GB fiber ports or to existing 1GB copper ports on the Cisco Nexus 7000 in the TIC Gateways.	
3.10.11. The systems shall retain all collected event data for three (3) years at each location.	
4. Pre-Packaged Content and Capabilities for Security/SIEM Use Cases	
4.1. Shall be able to save search criteria for future use	
4.2. Existing searches shall be easily modified and new searches shall be able to be created ad-hoc	
4.3. Each search has automatic, configurable assignment of severity, owner, and status	
4.4. Flexible searching and alerting options (see section 8 on searching & alerting)	
4.5. Searches and visualizations covering multiple categories and technologies including:	
4.5.1. Authentications, usage of default accounts, malware, endpoint changes, patch levels, firewalls, IDS, vulnerability scans, web proxies, abnormal HTTP-based activity, and port/protocol changes	
4.6. All reports and dashboards can be fully modified (see section 9 on reporting)	
4.7. Reports and dashboards all support drill-down capabilities to get from a high-level dashboard to a raw event	
4.8. Reports and dashboards contain simple filtering options and form boxes to help users narrow down data to what is of interest to them	
4.9. Incident review/workflow framework for reviewing and processing incidents	

4.9.1. Details on each incident including:	
4.9.1.1. The raw event(s) that constitute the incident	
4.9.1.2. The workflow history of the event	
4.9.1.3. Drop-down options on each relevant field that make it easy to pivot the investigation down a different path	
4.9.2. Shall be able to manually change incident severity, owner, and status, as well as add notes to an incident	
4.10. Shall be able to leverage external data sources to enrich raw events, add context, and create more specific correlation searches (see section 7 on external data sources)	
4.10.1. Employee information (e.g., Active Directory/LDAP)	
4.10.2. Asset information (e.g., hostname, IP address, system function, system owner, etc.)	
4.10.3. Lists of prohibited services/processes/IPs/ports/protocols	
4.10.4. Ability to add new threat intelligence feeds, whether open-source or proprietary	
4.10.5. Other arbitrary lists (e.g. usernames or email addresses)	
4.11. Includes support for custom applications to collect external data sources	
4.12. Pre-configured field extractions for at least the following log data sources:	
4.12.1. Palo Alto Firewalls	
4.12.2. Cisco Ironport	
4.12.3. Cisco Network Access Control	
4.12.4. Cisco Access Control System	
4.12.5. Cisco IOS	
4.12.6. Cisco ASA Firewalls	

4.12.7. Cisco ASA VPN	
4.12.8. IBM ISS IPS	
4.12.9. SourceFire Defense Center	
4.12.10. F5 Application Security Module	
4.12.11. F5 DNS Logs	
4.12.12. F5 Global Traffic Manager	
4.12.13. Citrix Netscaler	
4.12.14. UNIX Authentication Logs	
4.12.15. Windows Authentication Logs	
4.12.16. Netapp Filer	
4.12.17. McAfee EPO	
4.12.18. IBM Endpoint Manager	
5. Satisfies Compliance Use Cases	
5.1. Meets regulatory requirements around log management, retention, review, and continuous monitoring.	
5.2. Dashboards and reports can be created to measure compliance with any technical control trackable in machine data	
5.3. Can be used for major regulations and frameworks including:	
5.3.1. PCI	
5.3.2. GLBA	
5.3.3. HIPAA	
5.3.4. FISMA	
5.3.5. SOX	
5.3.6. NERC	
5.3.7. US state privacy regulations	
5.3.8. NIST 800-53	
5.3.9. ISO 27002	

5.3.10. COBIT	
5.3.11. SSAE 16	
5.4. Can be used to satisfy internal audit requests and auditor ad-hoc information requests	
6. Shall Index Any Machine Data or Log Files From Any Source	
6.1. Shall index human-readable machine data from any app, OS, device, or system whether virtual, physical, or cloud-based	
6.2. Shall accommodate new data sources or changes in the log format of an existing data source	
6.3. Shall index and correctly associate multi-line or complex event logs	
6.4. M Shall ust be able to conduct some level of intelligent, automatic field extraction from log data	
6.5. By default, Shall be able to ingest and index arbitrary machine data log sources and perform field extractions for at least the following categories of devices:	
6.5.1. Firewalls	
6.5.2. Intrusion Detection System / Intrusion Prevention System	
6.5.3. Authentication system (including LDAP and Active Directory)	
6.5.4. Data Loss Prevention	
6.5.5. Anti-malware	
6.5.6. Automated malware analysis tools	
6.5.7. Web security or web proxy	
6.5.8. Email security	
6.5.9. Vulnerability scanners	
6.5.10. File integrity monitoring	
6.5.11. Web application firewalls	
6.5.12. Operating system logs (endpoints and	

servers)	
6.5.13. Email server	
6.5.14. Web server	
6.5.15. DHCP/DNS	
6.5.16. VPN	
6.5.17. Network Flows (NetFlow, IPFIX, etc)	
6.5.18. PCAP files	
6.5.19. Networking devices (routers, switches)	
6.5.20. Databases and mainframes	
6.5.21. NAS devices and filers	
6.5.22. Hypervisor and virtual machine logs	
6.5.23. Service desk	
6.5.24. Call records	
6.5.25. Mobile devices and mobile device management systems	
6.5.26. Server and Endpoint Management tools	
6.5.27. SCADA devices	
6.5.28. Industrial control systems	
6.5.29. Manufacturing systems	
6.5.30. Physical badge data	
6.5.31. Hosted VM environments (Amazon Web Services, Rackspace, etc)	
6.5.32. Cloud-based applications (Box, Salesforce.com, etc)	
6.5.33. Social media (Twitter, Facebook, Foursquare, etc)	
6.5.34. Web analytics	
6.5.35. ERP and CRM	
6.5.36. Radio Frequency Identification (RFID)	
6.5.37. Global Positioning System (GPS)	
6.5.38. Custom applications	

6.6. By default, shall be able to ingest and index arbitrary machine data log sources, and perform field extractions for at least the following specific devices:	
6.6.1. Palo Alto Firewalls	
6.6.2. Cisco Ironport	
6.6.3. Cisco Network Access Control	
6.6.4. Cisco Accesss Control System	
6.6.5. Cisco IOS	
6.6.6. Cisco ASA Firewalls	
6.6.7. Cisco ASA VPN	
6.6.8. IBM ISS IPS	
6.6.9. SourceFire Defense Center	
6.6.10. F5 Application Security Module	
6.6.11. F5 DNS Logs	
6.6.12. F5 Global Traffic Manager	
6.6.13. Citrix Netscaler	
6.6.14. UNIX Authentication Logs	
6.6.15. Windows Authentication Logs	
6.6.16. Netapp Filer	
6.6.17. McAfee EPO	
6.6.18. IBM Endpoint Manager	
6.7. Shall be able to encrypt communications to the system, cache data, load balance data to different components, and send data via TCP	
6.8. Ability to receive data via a wide range of agent-based and agent-less mechanisms including:	
6.8.1. Syslog	
6.8.2. TCP or UDP	
6.8.3. SNMP events	
6.8.4. XML	
6.8.5. CSV	

6.8.6. JSON	
6.8.7. WMI	
6.8.8. Directly pointing to log files over the network or on a device	
6.8.9. Custom inputs	
6.8.9.1. Scripted inputs	
6.9. Ability to directly connect to any SQL database table(s) and extract the contents for indexing	
6.10. Ability to import raw data from Hadoop for indexing	
7. Shall Enrich Indexed Data With External Sources to Add Context or Information	
7.1. Newly indexed data shall be applied to previously indexed data to facilitate searching and reporting going back days, months, or years	
7.2. Shall take raw, indexed data and use it to perform lookups against any value in a database or CSV file	
7.3. Integrates with corporate directories (AD, LDAP, etc.) to extract employee information including:	
7.3.1. Employee user names, first, last, phone, manager, department, location, if privileged, if on watchlist, start and end dates, etc.	
7.4. Integrates with asset databases to extract asset information including:	
7.4.1. Device host name, IP, MAC, location, if containing confidential data, if relevant to a given regulation, etc.	
7.5. Ability to easily integrate with any third-party, free or commercial, human-readable data feed	
8. Flexible Search and Alerting Capabilities	
8.1. Shall be able to sustain search speeds with the following parameters:	

8.1.1. Shall be able to run at least 50 concurrent user-spawned on demand searches (without queuing), each of which is querying 30 days' worth of data across all indexed data (120TB, scalable to 960TB), and return the results for each within 20 minutes of launch, while still meeting all other requirements"	
8.1.2. Ability to perform "result caching" and save summary data to flat files or separate database(s) to expedite searches	
8.1.3. Ability to search and alert on both raw data and summary data	
8.2. Ability to do full-text search on any field in the indexed data based on:	
8.2.1. Keywords	
8.2.2. Time ranges	
8.2.2.1. Specific or relative time windows down to the month/day/hour/minute/second	
8.2.3. Boolean logic (and, or, not, etc.)	
8.2.4. Regular expressions	
8.2.5. Wild card syntax	
8.2.6. Mathematical and statistical operations including:	
8.2.6.1. Count of occurrences, distinct count of occurrences, sum	
8.2.6.2. Most common values or least common values of a field	
8.2.6.3. Minimum, maximum	
8.2.6.4. Average, mean, mode, median	
8.2.6.5. Standard deviation, variance	
8.2.6.6. The identification of anomalous values in results that may be irregular, or uncommon	
8.2.6.7. The statistical correlation between fields	
8.2.6.8. Clustering of events together based on their similarity to each other as a single event	

8.2.6.9. Truncate outlying numerical values in selected fields to assist in statistical correlation	
8.2.6.10. First and last seen value	
8.2.6.11. Percentile	
8.2.6.12. Predicted values (search that looks at historical data to mathematically predict future values)	
8.2.6.13. Perform a union, diff, or intersection of individual or multiple search results	
8.2.6.14. Search for relationships between pairs of fields by comparing the values of one field to a reference field and value pair	
8.3. Ability to set a baseline and then apply the above search logic to find outliers/anomalies from the baseline	
8.4. Searches enable the user to data-mine based on who, what, when and where	
8.5. Searches can easily be saved, shared, and modified	
8.6. Searches can be real time or scheduled	
8.7. Ability to run multiple concurrent searches	
8.8. Searches can be applied directly to raw data stored externally in Hadoop HDFS file systems and the results made available for advanced visualizations	
8.9. Scheduled searches can be scheduled for any time	
8.10. Real-time alerting capabilities on a per-search basis that can:	
8.10.1. Send an email	
8.10.2. Add to a RSS feed	
8.10.3. Execute a custom script	
8.10.3.1. Scripts can act as “middleware” enabling automated remediation actions involving different vendor products	
8.10.4. Be configured so not every event that meets the search parameters results in an alert action	

8.11. Searches can include multiple sub-searches to include outer and inner join statements.	
8.12. No fixed maximum on the number of searches or alerts that can be run	
8.13. No fixed maximum on the number of results that can be returned by a search	
8.14. No fixed maximum on the number of results that can be exported	
9. Flexible Reporting Functionality	
9.1. The solution shall enable the easy creation of a wide range of visualizations (not limited to fixed, pre-canned reports)	
9.2. Native visualizations shall include:	
9.2.1. Tables	
9.2.2. Time charts	
9.2.3. Line charts	
9.2.4. Bar charts	
9.2.5. Area charts	
9.2.6. Pie charts	
9.2.7. Scatterplot charts	
9.2.8. Radial, filler, and marker gauges	
9.2.9. Geo-IP maps	
9.3. Visualizations shall have the ability to update in real-time	
9.4. Visualizations shall be able to make clear outliers/anomalies in need of further investigation	
9.5. Visualizations shall all support drill-down, click-through capabilities to get from visual summaries to raw events	
9.6. Drag and drop user interface to build custom reporting dashboards requiring only a basic understanding of the search language and data format	
9.7. For all charts, there shall be an easy ability to change	

titles, legends, and axis labels and settings	
9.8. Charts shall support logarithmic scale plotting	
9.9. Ability to easily print events, tables, and visualizations	
9.10. Ability to convert dashboards into PDF files and schedule them to be emailed to users	
9.11. Ability to integrate with external visualization frameworks and options (e.g. D3, Tableau, etc.) for additional visualizations	
9.12. No fixed maximum on the number of reports or dashboards that can be created	
9.13. No fixed maximum on the number of searches or results used to populate a report or dashboard	
10. The Solution shall be Secure and Maintain Data Integrity	
10.1. Flexible Roles Based Access Control (RBAC) for controlled user and API access	
10.1.1. Enables restricted access to specific data sources, data types, time periods, specific views, reports or dashboards	
10.2. Authentication and authorization integration with Active Directory, eDirectory, and other LDAP-compliant implementations	
10.3. Integration with enterprise single sign-on solutions enabling pass-through authentication of third party credentials	
10.4. Real-time remote indexing of data Secure data stream access and distributed functionality via SSL/TCP	
10.5. Block-signs events with a digital signature to demonstrate integrity of the indexed data	
10.6. Event hashing at index time to determine at search time if events have been tampered with	
10.6.1. Shall provide a means to recover data if event tampering does occur	

10.7. Monitors its own configurations and usage to maintain a complete, digitally signed audit trail of who is accessing the system, what searches they are running, what reports they are viewing, what configuration changes they are making	
11. Open Platform	
11.1. Offers a REST API to expose all indexed data, search commands, and functionality to external systems, applications, or dashboards	
11.2. Offers the following Software Development Kits (SDKs) on top of the API, at a minimum::	
11.2.1. Python	
11.2.2. Java	
11.2.3. JavaScript	
11.2.4. PHP	
11.2.5. Ruby	
11.2.6. C#	
11.3. Shall be able to create views using XML	
11.4. Supports integration with third-party and custom applications	
11.5. All system configurations are configurable via the UI, CLI, or files on the file system, enabling granular changes and customization	
11.6. All reports and dashboards are editable either via the UI or underlying XML files, enabling flexible editing	
11.7. Ability to easily forward on data to any external system or logging tool	
11.7.1. At index time, raw data can be forwarded as syslog via TCP or UDP, or as raw TCP	
11.7.2. At search time, the solution shall be able to forward selected, transformed, and/or enriched events as a file, or as syslog over TCP or UDP	

5.5 SOFTWARE LICENSES

The Contractor shall provide perpetual software licenses that cover patches and version updates throughout the period of performance of the contract for the turn-key solution. The Contractor shall provide perpetual software user licenses that will cover approximately 150 NSOC personnel and shall be expandable up to 10% per PoP.

Deliverable:

A. Software Licenses

B. Software User Licenses

5.6 ACCREDITATION & AUTHORIZATION (A&A) DOCUMENTATION SUPPORT

The Contractor shall provide documentation for the Government's A&A activities in accordance with the following guidelines:

- The Office of Management and Budget (OMB) Circular A-130, Appendix III; Security of Federal Information Resources.
- National Institute of Standards and Technology (NIST) Special Publication, (SP) SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations.
- National Institute of Standards and Technology (NIST) Special Publication, (SP) SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations.

The Contractor shall create and deliver the A&A documentation as defined in the Accreditation Requirements Guide (see Attachment 2).

Deliverables:

A. A&A Documentation

5.7 ENGINEERING (IMPLEMENTATION) SERVICES

The Contractor shall provide a detailed operational design documentation to include the overall architecture design with the number of devices to be installed in each location. The Contractor shall provide all documentation detailing the configuration and implementation of the overall systems. The Contractor shall perform all configurations of the systems prior to deployment to each location. The Contractor shall provide escalation services throughout the deployment phase of the systems.

5.7.1 ENGINEERING AND SUPPORT SERVICES

The Contractor shall provide a dedicated on-site Subject Matter Expertise (SME) to provide expert level knowledge on the integration or interoperability of the SIEM with IBM End Point Manager to provide support during implementation.

The SME shall perform the following tasks:

1. Integrate rules from the CDCO deployment into NSOC operational processes,
2. Develop integration strategies between the SIEM solution and the VA's current deployment of Tivoli Enterprise Manager,
3. Provide technical support to correlate device data feeds with SIEM tool.
4. Provide on-the-spot SIEM system troubleshooting.
5. Perform tasks and provide daily status to local CDCO manager.
6. Provide onsite technical engineering support for production installation in each of the four (4) TIC GWs and integration with CDCO.
7. Provide day-to-day operational documentation and support to include enhancing/updating SOPs, process development, reporting activities, user guides, and operational related documentation.

IBM Endpoint Manager is the remote management tool used by the VA Enterprise to deliver Managed Computer Support services to Windows and Mac computers receiving Standard Desktop Support.

***Requirements in section 5.7.1 are not required if Splunk is the presented solution.

Deliverables:

A. Detailed Design Documentation
B. Detailed Operational Design Documentation

5.8 ACCEPTANCE TESTING

The VA has concerns regarding the compatibility of the solution in the VA environment. To address these concerns, the VA will test the solution and proceed with the procurement as described in the VA's Test Acceptance Plan for SIEM (see Attachment 3). The Contractor shall deliver the solution to VA as described in the Special Shipping Instructions section below. The VA will compile a report documenting the findings and share with the Contractor.

5.9 IMPLEMENTATION

The Contractor configuration efforts shall take place in Martinsburg, WV. VA will conduct delivery efforts of SIEM equipment to the Martinsburg, WV facility (CRRC) and subsequently to the destination sites after configuration in completed. VA will ship the equipment to Martinsburg one site at a time. The Contractor shall stage and configure the equipment in Martinsburg one site at a time. For shipping instruction see "Special Shipping Instructions".

Implementation is defined herein as configuring and testing the SIEM solution to work with VA Network Systems/devices listed in TRM. The Contractor shall install and

configure, as part of the SIEM solution, the SIEM components to be deployed within the locations defined in this section.

Installation services for the Lab or production network will not commence until validated receipt of all hardware by the VA Project Manager. The Contractor shall initiate onsite installation and user acceptance testing for the Test Lab system located in Martinsburg, WV within 30 days of the VA confirming receipt of the product. The Contractor shall take no longer than 10 business days to complete installation (to include Contractor and VA testing) so the lab environment can be ready for VA user acceptance testing. The Contractor shall provide onsite technical engineering support for deployment immediately following successful testing in the lab.

The Contractor shall provide an integrated master schedule in MS Project that details how the Contractor intends to fulfill VA's implementation requirements within a 12-month time period with the following constraints:

- VA requires 45 days from delivery acceptance of hardware to process inventory control.
- VA requires 10 business days for Logistical coordination with Service Support Service Line Managers for field implementation.
- Contractors arriving onsite at VA facilities and VA Contractor facilities must have security clearance (as define in Section 6.2) prior to arrival.

The Contractor shall propose a Production installation schedule to include the locations identified below:

Gateway North Chicago, IL 60616	Gateway East Sterling, VA 20166
Gateway South Dallas, TX 75234	Gateway West San Jose, CA 95134

The Contractor shall provide SIEM software installation and configuration documentation, in Microsoft Word format, to include as-built and default installation and configuration:

- Default installation and configuration documentation for the primary management software.
- Default installation and configuration documentation for the database.
- Default installation and configuration documentation for the sensors/event collectors.
- Final "as-built" documentation of the VA's implementation of the primary management software, database, and sensor/event collectors as part of the Configuration Baseline.

The Contractor shall provide to the VA with the progress, status and logistics of the following items and document onto the BWARs (refer to Section 5.2.2):

- Delivery of product
- Installation of lab equipment
- Training
- Documentation
- Invoicing

Deliverable:

A. Contractor Proposed Integrated Master Schedule
B. SIEM Software Installation and Configuration Documentation

5.10 TRAINING

Training sessions shall be hands-on training and will be conducted in a VA classroom setting that allows instructor/ VA user audio and visual interaction for immediate feedback and discussion which is necessary for VA users to achieve understanding of the tasks and learning objectives. If classroom training is conducted, then training sessions shall be done at VA facilities.

5.10.1 Training shall address user level and advanced level training as follows:

5.10.1.1 User level training. User level training is required for all basic and advanced users of the product and shall provide deep visibility into network, user, and application activity. It shall provide information for users to learn how to navigate the SIEM to detect anomalies and unusual behavior. Upon completion of the course, users must be able to identify and investigate threats and attacks.

5.10.1.2 Advanced user training. Advanced user level training is required for all advanced users of the product. Advanced users must first complete the user level training, and must also complete training for advanced users/administrator. Upon completion of the course, Advanced users and administrators must be able to create Universal DSM and create event, flow and anomaly rules; analyze the offenses created by rules and, if necessary, fine-tune them.

5.10.2 All electronic training materials or recordings of user and advanced user training shall be provided for reference.

5.10.3 TRAINING SESSION REQUIREMENTS

The Contractor shall provide a total of six (6) training sessions for the NSOCs at Hines, IL and Martinsburg, WV. These six (6) training sessions shall consist of two (2) basic and one (1) advanced session per NSOC location. Advanced User Training shall accommodate up to ten (10) users per session. Basic User Training shall accommodate up to twenty-five (25) users per session. Training is defined at PWS paragraph 5.9. The initial six (6) training sessions shall occur within thirty (30) days

after the Lab installation is complete in Martinsburg, WV and user acceptance testing is completed.

***Training is not required if Splunk is the presented solution.

Deliverables:

A. Training Package
B. Electronic Training Package

5.11 PRODUCT SUPPORT SERVICES

The Contractor shall provide system maintenance support 24 hours/day, 7 days/week, and 365 days/year coverage of United States-based telephone technical support to answer questions and issue resolutions. The Contractor shall provide a four (4) hour response time to deploy replacement for next day delivery.

Per VA 6500.3 media sanitation regulations, VA will not return any data storage media and memory under any circumstance. The Contractor shall provide software upgrades and patches as required. The Contractor shall provide system version upgrades, patches and code for the period of performance of the contract.

5.12 OPTION PERIOD 1

If the Option Period is exercised by VA, the Contractor shall perform tasks 5.5 and 5.11 throughout the duration of Option Period 1.

5.13 OPTION PERIOD 2

If the Option Period is exercised by VA, the Contractor shall perform tasks 5.5 and 5.11 throughout the duration of Option Period 2.

5.14 SHIPPING INSTRUCTIONS

Primary Ship To:

Name: Demetrius Lowery
Address: 7100 Old Landover Road, Building C
Landover, MD 20785
Voice: 202-461-6351
Email: Demetrius.Lowery@va.gov

VA NSOC POC:

Name: Jonathan Hiller
Address: CRRC, 221 Butler Ave., Bldg. 511
Martinsburg, WV 25125
Voice: (304) 262-5287
Email: Jonathan.Hiller2@va.gov

Security Information and Event Management (SIEM) Solution
TAC Number: TAC-14-13183

Special Shipping Instructions:

Prior to shipping, Contractor shall notify both Primary Ship To POC and VA NSOC POC, by phone and followed by email, of all incoming deliveries including line-by-line details for review of requirements. Contractor cannot make any changes to the delivery schedule at the request of the Site POC.

The Contractor shall package like type hardware together. Contractors must coordinate deliveries with above noted POCs before shipment of hardware to ensure sites have adequate storage space. All shipments, both single and multiple container deliveries, will bear the VA Purchase Order number on external shipping labels and associated manifests or packing lists. In the case of multiple container deliveries, a statement readable near the VA PO number will indicate total number of containers for the complete shipment (ex. "Package 1 of 2"), clearly readable on manifests and external shipping labels.

Packing Slips/Labels and Lists shall include the following:

IFCAP PO # _____ (i.e., 166-E11234)
Total Number of Containers: Package ___ of ___. (i.e., Package 1 of 3)

Primary tasks will be performed at the following VA facilities:

Department of Veterans Affairs
VA NSOC
Capital Region Readiness Center
221 Butler Avenue (Building 511)
Martinsburg, WV 25405

Department of Veterans Affairs
Hines ITC
Bldg. 215 Rm 147J, ,
1st Ave. North of 22nd St.
Hines, IL 60141

VA Gateways located at Vendor facilities:

Gateway North Qwest Communications 350 E Cermak Road 7th Floor, Chicago, IL 60616 ATTN: Veterans Affairs	Gateway South AT&T 11830 Webb Chapel Road Ste 200, Dallas, TX 75234 ATTN: Site ID 17273
Gateway East Qwest Sterling 1 Cybercenter	Gateway West AT&T

22810 International Dr, Sterling, VA 20166 ATTN: Veterans Affairs	400 Holger Way, San Jose, CA 95134 ATTN: Site ID 17281

5.15 POINTS OF CONTACT

COR Contact Information:

Name: Glenn Fudge
Address: VA NSOC Capital Region Readiness Center
221 Butler Avenue (Building 511)
Martinsburg, WV 25405
Phone: 304-262-5238
Email: Glenn.fudge@va.gov

Project Manager Contact Information:

Name: Lucky Rabago
Address: 2301 E. Lamar Blvd., Suite 330
Arlington, TX 76006
Phone: 708-938-2710
Email: lucky.rabago@va.gov

Contracting Officer Contact Information:

Name: Carolyn Klein
Address: 23 Christopher Way Eatontown, NJ
Voice: 732-795-1165
Email: Carolyn Klein@va.gov

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

The Contractor shall support the VA Enterprise management framework. In association with the framework, the Contractor shall comply with OIT Technical Reference Model (One-VA TRM). One-VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain Enterprise applications. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. Architecture, Strategy, and Design (ASD) has overall responsibility for the One-VA TRM.

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directives issued by the Office of Management and Budget (OMB) on August

2, 2005 (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf) and September 28, 2010 (https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf). IPv6 technology, in accordance with the USGv6 Profile (NIST Special Publication (SP) 500-267 http://www-x.antd.nist.gov/usgv6/index.html), the Technical Infrastructure for USGv6 Adoption (http://www.nist.gov/itl/antd/usgv6.cfm), and the NIST SP 800 series applicable compliance (http://csrc.nist.gov/publications/PubsSPs.html) shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 users, and all internal infrastructure and applications shall communicate using native IPv6 operations. Information concerning IPv6 transition in addition to OMB/VA Memoranda can be found at https://www.voa.va.gov/.

The Contractor shall support VA efforts in accordance with the Project Management Accountability System (PMAS) that mandates all new VA IT projects/programs use an incremental development approach, requiring frequent delivery milestones that deliver new capabilities for business sponsors to test and accept functionality. Implemented by the Assistant Secretary for IT, PMAS is a VA-wide initiative to better empower the OIT Project Managers and teams to meet their mission: delivering world-class IT products that meet business needs on time and within budget.

6.2 POSITION/TASK RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

Position Sensitivity	**Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Security Suitability Program," Appendix A)
Low	**National Agency Check with Written Inquiries (NACI)** A NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.
Moderate	**Moderate Background Investigation (MBI)** A MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree.

Position Sensitivity	**Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Security Suitability Program," Appendix A)
High	**Background Investigation (BI)** A BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree.

The position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the Performance Work Statement are:

Position Sensitivity and Background Investigation Requirements

Task Number	N/A	Low/NACI	Moderate/MBI	High/BI
5.1	☒	☐	☐	☐
5.2	☒	☐	☐	☐
5.3	☒	☐	☐	☐
5.4	☒	☐	☐	☐
5.5	☒	☐	☐	☐
5.6	☒	☐	☐	☐
5.7	☐	☐	☒	☐
5.8	☐	☐	☒	☐
5.8.1.4	☒	☐	☐	☐
5.9	☒	☐	☐	☐
5.10	☒	☐	☐	☐

The Tasks identified above and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the particular Contractor individual will be working. The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each Contractor individual based upon the tasks on which the Contractor individual will be working, in accordance with their submitted proposal.

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
b. The Contractor shall bear the expense of obtaining background investigations.
c. Within three (3) business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations. The roster shall contain the Contractor's Full Name, Full Social Security Number, Date of Birth, Place of Birth, and individual background investigation level requirement (based upon Section 6.2 Tasks).
d. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
e. For a Low Risk designation the following forms are required to be completed: 1.OF-306 and 2. DVA Memorandum – Electronic Fingerprints. For Moderate or High Risk the following forms are required to be completed: 1. VA Form 0710 and 2. DVA Memorandum – Electronic Fingerprints. These should be submitted to the COR within 5 business days after award.
f. The Contractor personnel will receive an email notification from the Security and Investigation Center (SIC), through the Electronics Questionnaire for Investigations Processes (e-QIP) identifying the website link that includes detailed instructions regarding completion of the investigation documents (SF85, SF85P, or SF 86). The Contractor personnel shall submit all required information related to their background investigations utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP).
g. The Contractor is to certify and release the e-QIP document, print and sign the signature pages, and send them to the COR for electronic submission to the SIC. These should be submitted to the COR within 3 business days of receipt of the e-QIP notification email.
h. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
i. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or "Closed, No Issues" (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).

j. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
k. Failure to comply with the Contractor personnel security investigative requirements may result in termination of the contract for default.

GOVERNMENT RESPONSIBILITIES

The following information must be provided by the CO to the Contractor:

1. The Security Investigations Center (SIC) will require the following forms from the Contractor or the Contractor's personnel:
   a. For Low Risk: 1. OF-306 and 2. DVA Memorandum – Electronic Fingerprints. (The SF85 does not need to be uploaded because OPM is going paperless and the Contractor will complete this questionnaire online when the e-QIP link is sent.) (DVA Memorandum – Electronic Fingerprints is filled out by the VA Facility that took the electronic fingerprint.)
   b. For Moderate or High Risk: 1. VA Form 0710 and 2. DVA Memorandum – Electronic Fingerprints. (The SF85P does not need to be uploaded because OPM is going paperless and the Contractor will complete this questionnaire online.) (DVA Memorandum – Electronic Fingerprints is filled out by the VA Facility that took the electronic fingerprint.)
2. Upon receipt, the VA Office of Security and Law Enforcement will review the completed forms for accuracy, initiate the Contractor in e-QIP and send an email notifying the CO or COR and the Contractor personnel that they have been initiated in e-QIP.
3. The Contractor will then login to e-QIP to complete the questionnaire (SF85 or SF 85P), and then prints and signs the signature pages which are then turned in to the CO/COR. (Please be advised that the Contractor will need all the necessary information easily accessible as the website will time out and previously entered information can be lost if the application times out while it is being completed.)
4. The SIC will then upload the e-QIP signature pages to e-QIP and release the case file to OPM for investigation.
   l. The SIC will notify the CO and Contractor after adjudicating the results of the background investigations received from OMB.

6.2.2.1 **Required Contractor Security Documentation**

Contractor personnel are required to complete the forms identified in this section as a part of the screening process.

New Hire Required Security Documents
1- Office of Personnel Management (OPM) Optional Form 306, *Declaration of Federal Employment*
2- VA Form 0710, *Authorization for Release of Information*
3- VA Form, *Self-Certification for Continuous Service*
4- VA Memo, SIC Electronic Fingerprinting
5- VA Memo, Local Elevate Privileges ROB (optional as this is only required for elevated privileges)
6- SF85 Foreign Born Employees ONLY

In addition, Contractor personnel are required to complete the following training

- TMS training
  - VA Privacy and Information Security Awareness and Rules of Behavior (mandatory for all)
  - Network Administrator: Your Role in IT Security (for elevated privileges ONLY)
  - System Administrator: Your Role in IT Security (for elevated privileges ONLY)
- OPM eQIP

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: MS Word 2000/2003/2007/2010, MS Excel 2000/2003/2007/2010, MS PowerPoint 2000/2003/2007/2010, MS Project 2000/2003/2007/2010, MS Access 2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

6.4 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Performance Levels for Objectives associated with this effort.

Performance Objective	***Performance Standard***	***Acceptable Performance Levels***

Security Information and Event Management (SIEM) Solution
TAC Number: TAC-14-13183

Performance Objective	*Performance Standard*	*Acceptable Performance Levels*
1. Technical Needs	***Shows understanding of requirements*** ***Efficient and effective in meeting requirements*** ***Meets technical needs and mission requirements*** ***Offers quality services/products***	***Satisfactory or higher***
A. Effective Communication	***No less than 3 contacts per week from Contractor***	***100% of the time***
B.Response to VA Query	***Responses received within 4 business hours of request***	***95% of the time measured on a monthly basis***
2. Project Milestones and Schedule	***Quick response capability*** ***Products completed, reviewed, delivered in timely manner*** ***Notifies customer in advance of potential problems***	***Satisfactory or higher***
3. Project Staffing	***Currency of expertise*** ***Personnel possess necessary knowledge, skills and abilities to perform tasks***	***Satisfactory or higher***
4. Value Added	***Provided valuable service to Government*** ***Services/products delivered were of desired quality***	***Satisfactory or higher***

The Government will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable manner. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion. A Performance Based Service Assessment Survey will be used in combination with the QASP to assist the Government in determining acceptable performance levels.

6.5 FACILITY/RESOURCE PROVISIONS

The Government will provide office space, telephone service and system access when authorized contract staff work at a Government location as required in order to accomplish the Tasks associated with this PWS. All procedural guides, reference materials, and program documentation for the project and other Government applications will also be provided on an as-needed basis.

The Contractor shall request other Government documentation deemed pertinent to the work accomplishment directly from the Government officials with whom the Contractor has contact. The Contractor shall consider the COR as the final source for needed Government documentation when the Contractor fails to secure the documents by other means. The Contractor is expected to use common knowledge and resourcefulness in securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

VA will provide access to VA-specific systems/network as required for execution of the task via remote access technology (e.g. Citrix Access Gateway (CAG), site-to-site(S2S) VPN, or VA Remote Enterprise Secure Compliance Update Environment (RESCUE)). This remote access will provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath, Primavera, and Remedy, including appropriate seat management and user licenses. The Contractor shall utilize Government-provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort. The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. For detailed Security and Privacy Requirements refer to **Error! Reference source not found.** and ADDENDUM B.

6.6 GOVERNMENT FURNISHED PROPERTY

For the IBM QRadar SIEM systems, VA will provide equipment racks, facility power, and facility network connectivity at each site.

VA will not provide any Information Technology (IT) equipment (i.e. laptops, mouse, air-card). Each person who will be located at VA offices will be provided space, desk, and telephones. All personnel will be given access to applicable VA documentation.

The Contractor-provided computer system shall be loaded with a VA NSOC-centric software suite. Contractor-provided computer systems shall be shipped to either the Martinsburg, WV or Hines, IL location and be addressed to the VA FTE (TBD after Contract award), at which time ownership of the Contractor-provided computer systems shall transfer to VA. If laptops are to be utilized, then it is incumbent upon the

Contractor to select equipment that is compatible with the current VA environment. The DELL (Precision or Latitude) are two examples of hardware that is currently compatible.

In accordance with the VA Media Sanitization policy, if the Contractor is utilizing his own computer equipment, then all hard drives shall be delivered to VA for destruction, at the conclusion of the contract; or upon demand; whichever comes first.

Security Information and Event Management (SIEM) Solution
TAC Number: TAC-14-13183

ADDENDUM A

A1.0 Cyber and Information Security Requirements for VA IT Services

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations. The Contractor's firewall and web server shall meet or exceed VA minimum requirements for security. All VA data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer as soon as possible. The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to certification and accreditation.

Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COR, CO, the Project Manager, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

Each documented initiative under this contract incorporates VA Handbook 6500.6, "Contract Security," March 12, 2010 by reference as though fully set forth therein. The VA Handbook 6500.6, "Contract Security" shall also be included in every related agreement, contract or order. The VA Handbook 6500.6, Appendix C, is included in this document as Addendum B.

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS), and will be tracked therein. The TMS may be accessed at https://www.tms.va.gov. If you do not have a TMS profile, then go to https://www.tms.va.gov and click on the "Create New User" link on the TMS to gain access.

Contractor employees shall complete a VA Systems Access Agreement if they are provided access privileges as an authorized user of the computer system of VA.

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at http://www.ea.oit.va.gov/index.asp in force at the time of issuance of this contract, including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP). VA reserves the right to assess contract deliverables for EA compliance prior to acceptance.

A2.1. VA Internet and Intranet Standards:

The Contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the Contractor's work includes managing, maintaining, establishing and presenting information on VA's Internet/Intranet Service Sites. This pertains, but is not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

A3.0 Notice of the Federal Accessibility Law Affecting All Electronic and Information Technology Procurements (Section 508)

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. Section 508 required the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards setting forth a definition of electronic and information technology and the technical and functional criteria for such technology to comply with Section 508. These standards have been developed and published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

Section 508 – Electronic and Information Technology (EIT) Standards

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: http://www.section508.gov and http://www.access-board.gov/sec508/standards.htm. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

_x_ § 1194.21 Software applications and operating systems
_x_ § 1194.22 Web-based intranet and internet information and applications
_x_ § 1194.23 Telecommunications products
_x_ § 1194.24 Video and multimedia products
_x_ § 1194.25 Self-contained, closed products
_x_ § 1194.26 Desktop and portable computers
_x_ § 1194.31 Functional Performance Criteria
_x_ § 1194.41 Information, Documentation, and Support

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the EIT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

A4.0 Physical Security & Safety Requirements

The Contractor and their personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property. Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed. It is the responsibility of the Contractor to park in the appropriate designated parking areas. VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

A5.0 Confidentiality and Non-Disclosure

The Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

The Contractor may have access to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard (“Security Rule”). Pursuant to the Privacy and Security Rules, the Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy

Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.

2. The VA Contracting Officer will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA Contracting Officer for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA Contracting Officer.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
    a. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
    b. Controlled access to system and security software and documentation.
    c. Recording, monitoring, and control of passwords and privileges.
    d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.

e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
h. Contractor does not require access to classified data.

8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
9. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

ADDENDUM B

APPLICABLE PARAGRAPHS TAILORED FROM: *THE VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE*, *VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010*

B1. GENERAL

Contractors, Contractor personnel, Subcontractors, and Subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

b. All Contractors, Subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e. The Contractor or Subcontractor must notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor's employ. The Contracting Officer must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

B3. VA INFORMATION CUSTODIAL LANGUAGE

1. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

2. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA information is returned to VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct onsite inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.

4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

5. The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/Subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

6. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

8. The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

9. The Contractor/Subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA minimum requirements. VA Configuration Guidelines are available upon request.

10. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA prior written approval. The Contractor/Subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

11. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or a Memorandum of Understanding-

Interconnection Service Agreement (MOU-ISA) for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

N/A

B5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

N/A

B6. SECURITY INCIDENT INVESTIGATION

a. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/Subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access.

b. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor’s notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/Subcontractor considers relevant.

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The Contractor, its employees, and its Subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/Subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

B7. LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract.

b. The Contractor/Subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

c. Each risk analysis shall address all relevant information concerning the data breach, including the following:

1) Nature of the event (loss, theft, unauthorized access);
2) Description of the event, including:

a) date of occurrence;

b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;

3) Number of individuals affected or potentially affected;

4) Names of individuals or groups affected or potentially affected;

5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;

6) Amount of time the data has been out of VA control;

7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);

8) Known misuses of data containing sensitive personal information, if any;

9) Assessment of the potential harm to the affected individuals;

10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and

11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

d. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

1) Notification;
2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
3) Data breach analysis;
4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

B8. SECURITY CONTROLS COMPLIANCE TESTING

N/A

B9. TRAINING

a. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems;
2) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* training and annually complete required security training;
3) Successfully complete *Privacy and HIPAA Training* if Contractor will have access to PHI;
4) Successfully complete the appropriate VA privacy training and annually complete required privacy training; and
5) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access

b. The Contractor shall provide to the contracting officer and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.