PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS
Office of Information & Technology
Network and Security Operations Center (NSOC)

Security Incident Event Management (SIEM)

Date: April 3, 2015
TAC-FY15-20511
PWS Version Number: 1.3

Contents

1.0 BACKGROUND

The mission of the Department of Veterans Affairs (VA), Office of Information & Technology (OI&T), Network and Security Operations Center (NSOC) is to provide benefits and services to Veterans of the United States. In meeting these goals, OI&T strives to provide high quality, effective, and efficient Information Technology (IT) services to those responsible for providing care to the Veterans at the point-of-care as well as throughout all the points of the Veterans' health care in an effective, timely and compassionate manner. VA depends on Information Management/Information Technology (IM/IT) systems to meet mission goals.

VA 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 VA 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 United States its' territories, VA facilities in other countries supporting large veteran populations (Philippines), and U.S. military communities in Asia and Europe. The infrastructure consists of Intrusion Prevention System (IPS) devices; host servers; desktops/laptops; and routers and switches. The VA also utilizes other network devices and tools such as: firewalls, Domain Name System (DNS) Blackhole, Access Control Servers, Domain Name System Security Extensions (DNSSEC), Cisco firewalls, Palo Alto NextGen firewalls, Network Intrusion Prevention and Detection systems, Anti-Virus, Host Based Intrusion Prevention Systems, Network Discovery, Compliance Scanning, Vulnerability Scanning and ePolicy Orchestrator (ePO) servers to secure the VA network. These network and security devices and tools are deployed in a distributed architecture that is centrally monitored and managed from VA NSOC organizational units in Martinsburg, WV and Hines, IL.

As mandated in OMB memorandum M-14-03, the VA NSOC is required 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, large segments of the VA have deployed the International Business Machines (IBM) QRadar Security Information and Event Management (SIEM) solution in the VA's Corporate Data Centers Operations (CDCO) in Austin, TX; Hines, IL; Philadelphia, PA; Martinsburg, WV; and Quantico, VA; Financial Service Center, Austin; DISA DECC, Brooklyn; DISA DECC, Warner-Robbins as well as in the "cloud" facilities and business partner gateways. Additionally the VA has a large deployment of Splunk currently used as the centralized logging solution for all devices hosted in each of the four Trusted Internet Connection (TIC) gateways. Additionally, Regional implementations are in the process of being deployed as the centralized logging solution for regional servers not already included in VA data centers. VA is also making use of the Microsoft System Center Operation Manager (SCOM) solution to assist in audit log collection requirements at a number of VA locations. These solutions should be considered integral components of the existing VA infrastructure.

The SIEM architecture will support VA NSOC's mandate to manage, protect and monitor the cyber security posture of the entire VA Enterprise. This SIEM will augment VA NSOC's ability to perform analyses of cyber security events; 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 and reporting, patch distribution and remediation planning.

2.0 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement, 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 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013
4. 10 U.S.C. § 2224, "Defense Information Assurance Program"
5. Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Development (CMMI-DEV), Version 1.3 November 2010; and Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Acquisition (CMMI-ACQ), Version 1.3 November 2010
6. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
7. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
8. VA Directive 0710, "Personnel Suitability and Security Program," June 4, 2010, http://www1.va.gov/vapubs/
9. VA Handbook 0710, Personnel Suitability and Security Program, September 10, 2004, http://www1.va.gov/vapubs/
10. VA Directive and Handbook 6102, "Internet/Intranet Services," July 15, 2008
11. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
12. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," November 28, 2000
13. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
14. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
15. 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
16. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
17. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, , 2012

18. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” September 20, 2012
19. VA Handbook 6500.1, “Electronic Media Sanitization,” March 22, 2010
20. VA Handbook 6500.2, “Management of Data Breaches Involving Sensitive Personal Information (SPI)”, January 6, 2012
21. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring Of VA Information Systems,” February 3, 2014
22. VA Handbook, 6500.5, “Incorporating Security and Privacy in System Development Lifecycle” March 22, 2010
23. VA Handbook 6500.6, “Contract Security,” March 12, 2010
24. Project Management Accountability System (PMAS) portal (reference https://www.voa.va.gov/pmas/)
25. OI&T ProPath Process Methodology (reference https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=27) NOTE: In the event of a conflict, OI&T ProPath takes precedence over other processes or methodologies.
26. Technical Reference Model (TRM) (reference at http://www.va.gov/trm/TRMHomePage.asp)
27. National Institute Standards and Technology (NIST) Special Publications (SP)
28. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008
29. VA Directive 6300, Records and Information Management, February 26, 2009
30. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
31. OMB Memorandum, “Transition to IPv6”, September 28, 2010
32. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, February 17, 2011
33. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 20, 2014
34. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
35. OMB Memorandum 05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005
36. OMB memorandum M-11-11, “Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011
37. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
38. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
39. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008

40. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
41. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
42. Draft NIST Special Publication 800-157, Guidelines for Derived PIV Credentials, March 2014
43. NIST Special Publication 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
44. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
45. VA Memorandum, VAIQ #7100147, Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12), April 29, 2011 (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
46. VA Memorandum, VAIQ # 7011145, VA Identity Management Policy, June 28, 2010 (reference Enterprise Architecture Section, PIV/IAM (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
47. IAM Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, PIV/IAM (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
48. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, October 1, 2013
49. OMB Memorandum M-08-05, “Implementation of Trusted Internet Connections (TIC), November 20, 2007
50. OMB Memorandum M-08-23, Securing the Federal Government’s Domain Name System Infrastructure, August 22, 2008
51. VA Memorandum, VAIQ #7497987, Compliance – Electronic Product Environmental Assessment Tool (EPEAT) – IT Electronic Equipment, August 11, 2014 (reference Document Libraries, EPEAT/Green Purchasing Section, https://www.voa.va.gov/documentlistpublic.aspx?NodeID=552)
52. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
53. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
54. Executive Order 13514, “Federal Leadership in Environmental, Energy, and Economic Performance,” October 5, 2009
55. Executive Order 13423, “Strengthening Federal Environmental, Energy, and Transportation Management,” January 24, 2007
56. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
57. VA Directive 0058, “VA Green Purchasing Program”, July 19, 2013
58. VA Handbook 0058, “VA Green Purchasing Program”, July 19, 2013

3.0 SCOPE OF WORK

The Contractor shall provide two independent autonomous production-ready centralized Security Information and Event Management (SIEM) systems that include hardware, software and licensure to collect and manage the metadata for security information event data. “System” is defined here as the working solution that includes all elements working together to satisfy the requirements herein. One system (Production system) shall reside in the four Trusted Internet Connection (TIC) environments. The second system (Test lab system) shall reside in the Test lab located at Martinsburg, WV. The Contractor shall provide installation, training, professional engineering services, 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.

Any work at the Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO).

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.

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 VA facilities located in the VA Martinsburg, WV facility (221 Butler Ave, Bldg. 511, Martinsburg, WV 25405). Work may be performed at remote locations with prior approval of the Contracting Officer's Representative (COR).

4.3 TRAVEL

The Government does not anticipate travel under this effort

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.1 PROJECT MANAGEMENT

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall deliver a Contractor Project Management Plan (CPMP) detailing the Contractor's approach, timeline and tools to be used in execution of the contract. 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 CPMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks and resource support. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. 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 also include the following four elements:

a) 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.
b) Schedule Management Plan 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.
c) Communication Management Plan identifies the formal communication methodology for the project.
d) Risk Management Plan the Contractor shall document foreseeable risks and a response plan to mitigate those risks.

The initial baseline CPMP shall be concurred upon and updated in accordance with Section B of the contract. The Contractor shall update and maintain the VA PM approved CPMP throughout the period of performance.

The Contractor shall support weekly Project Status Meetings (can be virtual) from the inception of the delivery order throughout the period of performance. The Contractor shall be prepared to discuss any concerns and issues identified in each Bi-Weekly Status Report. At the conclusion of each meeting, the Contractor shall prepare the minutes summarizing the discussion items.

Deliverables:

A. Contractor Project Management Plan

5.1.2 REPORTING REQUIREMENTS

The Contractor shall provide the Contracting Officer's Representative (COR) with Bi-Weekly Progress Reports in electronic form in Microsoft Word and Project formats. The report shall include detailed instructions/explanations for each required data element, to ensure that data is accurate and consistent. These reports shall reflect data as of the last day of the preceding 2 week period.

The Bi-Weekly Progress Reports shall cover all work completed during the reporting period and work planned for the subsequent reporting period. The report shall also identify any problems that arose and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving the issue. The Contractor shall monitor performance against the CPMP and report any deviations. It is expected that the Contractor will keep in communication with VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

Deliverables:

A. Bi-Weekly Progress Report

5.1.3 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 and VA COR with communications of project activities; manage risk, cost, and schedule. 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 delivery order 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 the necessary security clearances and have properly coordinated facility access well in advance of the date access is needed; and

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

5.2 GENERAL SIEM REQUIREMENTS

The Contractor shall provide two independent autonomous production-ready Centralized SIEM systems that include SIEM hardware, SIEM software, third party software, and licensure to collect and manage metadata for security information event data. Raw log collection will be managed by VA NSOC logging solution externally to the proposed SIEM. The SIEM will receive structured data (metadata only) pertaining to the raw logs and perform management and correlation. The Production SIEM system shall reside in the four Trusted Internet Connection (TIC) Gateways environment with sensors and management software instances (refer to Section 5.9 for locations).

The proposed solution shall be an autonomous solution managed by VA NSOC personnel. The proposed solution shall seamlessly integrate with existing SIEM technologies (QRadar and Splunk) deployed in the VA enterprise including VA Data Centers (DC) and OIT Regional SIEM/ Log Aggregation deployments across the enterprise. The proposed solution shall integrate with architected solutions within VA DCs in such a manner as to provide the VA NSOC with access to all SIEM data hosted across all enterprise SIEM, log aggregation and analysis solutions.

The Contractor shall deploy the Production system within the VA-NSOC segment of the enterprise and provide centralized monitoring and lab capabilities at VA NSOC locations in Hines and Martinsburg. (See Attachment A, "SIEM Architecture Diagram"). The Contractor shall provide a Production system that provides 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.

The Contractor shall provide a Test lab system that will reside in Martinsburg, WV and be configured to replicate the centralized 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 Test lab system shall have the ability to process 30,000 events per second.

The proposed Production System 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 components 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 including the following:

a. Estimated bandwidth based on proposed architecture

b. Storage volume based on proposed architecture

c. Hardware specifications

d. Licensing model

The Contractor shall deliver a SIEM solution that does not and will not contain any code that will, upon the occurrence or the nonoccurrence of any event, disable or reduce functionality or performance of SIEM solution provided by the Contractor. Such code includes but is not limited to a computer virus, restrictive key, node lock, time-out or other function, whether implemented by electronic, mechanical, or other means, which limits or hinders the use or access to any computer software based on residency on a specific hardware configuration, frequency of duration of use, or other limiting criteria. If any such code is present, as a result of a disabling caused by such code, the Contractor shall, at no cost, remove such code within a minimum of four hours from receipt of the Government's notice of the presence of such code. Inability of the Contractor to remove the disabling software code will be considered a material breach of the delivery order and the Government may exercise its right to terminate for default. Alternatively, the Government reserves the right to remove the code in lieu of termination.

The systems shall comply with VA Handbook 6500, and be compatible with VA Technical Reference Model (TRM) components and Federal Trusted Internet Connection (TIC) Reference Architecture 2.0 requirements.

5.3 SIEM SOLUTION REQUIREMENTS

The SIEM Solution shall satisfy all of the technical requirements listed in Attachment B System Technical Requirements.

5.4 SOFTWARE LICENSES

The Contractor shall provide software licenses that cover patches and version updates throughout the period of performance of the delivery order for the turn-key solution. The Contractor shall provide software user licenses that will cover a minimum of 180 simultaneous VA NSOC personnel.

Deliverables:

A. Software Licenses
B. Software User Licenses

5.5 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 800-53R4, 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 C).

Deliverables:

A. A&A Documentation

5.6 ENGINEERING (IMPLEMENTATION) SERVICES

The Contractor shall perform all configurations of the systems prior to deployment to each location including the Test lab. The Contractor shall provide escalation services throughout the deployment phase of the systems.

5.6.1 SUBJECT MATTER EXPERT

The Contractor shall provide a dedicated on-site Subject Matter Expert (SME) at the NSOC facility in Martinsburg, WV for the base year period to provide expert level knowledge during the Acceptance Testing (Section ??.??) as well as on system management, rule management, data analysis, and reporting.

The SME shall perform the following tasks:

1. Provide support and system expertise during the initial system Acceptance Testing
2. Integrate rules from the CDCO deployment into VA NSOC operational processes.
3. Develop integration strategies between the SIEM and other security tools in the enterprise.
4. Provide technical support to correlate device data feeds with the SIEM tool.
5. Provide technical support to activities requiring change approval. The VA employs strict change control processes that include technical and security reviews as well as approval and authorization boards. The dedicated on-site Subject Matter Expert (SME) for the base year shall be integral and engaged with this activity, being responsible for providing supporting details required for the approving authorities to make informed decisions.
6. Provide on-the-spot SIEM system troubleshooting.
7. Provide onsite technical engineering support for production installation in each of the four TIC GWs.
8. Provide day-to-day operational documentation and support to include enhancing/updating Standard Operating Procedures (SOPs), process development, reporting activities, user guides, and operational related documentation.

5.6.2 INITIAL SYSTEM DELIVERY

The Contractor shall ship the equipment and components for one of the TIC environments (Section 5.6.3) to be tested to Landover, MD. Shipment shall be coordinated with the VA PM. The Contractor configuration efforts shall take place in Martinsburg, WV. VA will conduct shipping efforts of SIEM equipment to the Martinsburg, WV Capital Region Readiness Center (CRRC) facility. VA will ship the equipment to Martinsburg one site at a time. The Contractor shall stage, fully configure and implement the equipment in Martinsburg one system at a time. Implementation is defined herein as configuring the SIEM to work with VA Network Systems/devices listed in TRM.

Installation services for the test lab or production network will not commence until validated receipt of all hardware by the VA Project Manager and said hardware's arrival in Martinsburg.

The Contractor shall initiate onsite installation and staging of the first Production system to be tested in Martinsburg, WV within 30 days of the VA validated receipt of the equipment. The Contractor shall take no longer than 10 business days to complete installation (not including time for VA shipping activities) so the test lab environment can be ready for VA acceptance testing as set forth in PWS paragraph 5.6.3. Upon completion of implementation of the Production systems the Contractor shall send a written notice to the COR when the Production system is ready for VA test and acceptance. The Contractor provided SME (section 5.6.1) shall provide onsite technical engineering support for all VA performed Acceptance Testing.

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 from date of award with the following constraints:

a) VA requires 45 days from delivery acceptance of hardware to process inventory control, validated receipt of all hardware and ship to Martinsburg, WV.
b) Contractors arriving onsite at VA facilities and VA Contractor facilities shall have security clearance (as defined in Section 6.2) prior to arrival.
c) The Contractor shall take into consideration the acceptance testing period.

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

Martinsburg, WV	Hines, IL
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 detailed operational design documentation to include the overall architecture design with the number of devices to be installed for each individual system in each location. The Contractor shall provide detailed design documentation which includes all documentation detailing the configuration and implementation of the overall systems.

The Contractor shall provide SIEM Software Installation and Configuration Documentation, in Microsoft Word format, to include as-built and default installation and configuration:

a) Default installation and configuration documentation for the primary management software.
b) Default installation and configuration documentation for the database.
c) Default installation and configuration documentation for the sensors/event collectors.
d) 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.

Deliverables:

A. First Site TIC Gateway Production SIEM System
B. Integrated Master Schedule
C. Detailed Design Documentation
D. Detailed Operational Design Documentation
E. SIEM Software Installation and Configuration Documentation

5.6.3 ACCEPTANCE TESTING SUPPORT

VA shall perform Acceptance Testing on the Test Lab System and the first site production system in the Test Lab. VA will test each system's equipment and components and proceed with the procurement as described herein. VA will compile a report documenting the findings and share with the Contractor.

5.6.3.1 APPLICABLE CONDITIONS

The systems to be tested shall be ready for testing after the Contractor has configured the systems for the intended VA environments in accordance with Sections 5.2 and 5.3 of the PWS. The one system that shall be tested:

a) The equipment and components for one of the Trusted Internet Connection (TIC) Gateways environment and CRRC console. This shall include what is necessary to test, at a minimum, the full functionality of the SIEM utilizing only one TIC Gateway.

5.6.3.2 TESTING LOGISTICS

The Contractor shall provide to the COR written notice when the system for the TIC Gateways environment and CRRC console has been successfully implemented in the test lab at the CRRC in Martinsburg, WV. Testing shall take place in the test lab environment which is isolated from any production network for a period of 15 business days. Testing shall conclude in the live TIC production environment for a period of 15 business days. In the event the Contractor SME is required to perform corrective action on either of the test systems during the testing period, VA will commence a new testing period for the requisite 15 business days for both systems.

5.6.3.3 TEST AND ACCEPTANCE CRITERIA

VA shall test against the following: configuration; installation; and performing SIEM functions as required herein as well as against additional capabilities from the Contractor's proposed capabilities that have been incorporated into the final delivery order. The proposed solution shall be fully operational and not experience any downgraded performance or functionality during the testing period. The VA will compile a report documenting the findings and share with the Contractor. The Contractor, upon receipt of the report, shall have 15 business days to repair and/or replace any defects or non-conforming components.VA acceptance is conditioned upon error free operation of both the Test lab system and Production system for 15 business days.

5.7 ADDITIONAL SYSTEM DELIVERIES

Upon VA acceptance of the first TIC Gateway production system, the Contractor shall continue with the delivery and implementation of the remaining four SIEM systems in accordance with the Integrated Master Schedule from section 5.6.2. Upon VA verification of successful implementation of each system, VA shall deliver and install each system into the respective location.

Deliverables:

A. Test Lab SIEM System
B. Second TIC Gateway Site Production SIEM System
C. Third TIC Gateway Site Production SIEM System
D. Fourth TIC Gateway Site Production SIEM System

5.8 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.

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

Basic 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 shall be able to identify and investigate threats and attacks.

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

All electronic training materials or recordings of user and advanced user training shall be provided for reference. These materials are detailed in section 5.8.1.

5.8.1 TRAINING SESSION REQUIREMENTS

The Contractor shall provide a total of six (6) training sessions for the VA NSOC at Hines, IL and Martinsburg, WV. These six (6) training sessions shall consist of two (2) basic and one (1) advanced session per VA 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 5.10. The initial six (6) training sessions shall be scheduled and begin within thirty (30) days after the Test lab system installation is complete in Martinsburg, WV and VA has accepted both systems pursuant to Section 5.8.

The initial six (6) training sessions shall be scheduled and begin within thirty (30) days after the Test Lab system installation is complete in Martinsburg, WV and VA has accepted both systems pursuant to Section 5.8.

The Contractor shall provide a Training Package which shall consist of work books. The Contractor shall also provide an Electronic Training Package which shall include CDs.

Deliverables:

A. Training Package
B. Electronic Training Package

5.9 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. Support shall include routine system updates for hardware and software as well as any required repairs and equipment replacements. The Contractor shall provide a four hour response time after written notification from the COR to deploy replacement for next day delivery. The Contractor shall also provide and install all regular software/hardware upgrades/ updates into each SIEM system.

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 delivery order.

5.10 OPTION PERIOD 1

If the Option Period is exercised by VA, the Contractor shall perform tasks 5.9 throughout the duration of Option Period 1 to continue maintenance, licenses and technical support. The Contractor shall also provide and install all regular software/hardware upgrades/ updates into each SIEM system.

5.11 OPTION PERIOD 2

If the Option Period is exercised by VA, the Contractor shall perform tasks 5.9 throughout the duration of Option Period 2 to continue maintenance, licenses and technical support. The Contractor shall also provide and install all regular software/hardware upgrades/ updates into each SIEM system.

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 OI&T 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 shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are PIV-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), http://www.ea.oit.va.gov/EAOIT/OneVA/EAETA.asp, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/docs_design_patterns.asp. The Contractor shall ensure all Contractor delivered applications and systems are compliant with VA Identity Management Policy (VAIQ# 7011145), Continued Implementation of Homeland Security Presidential Directive 12 (VAIQ#7100147), and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document), located at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514. The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63-2, VA Handbook 6500 Appendix F, “VA System Security Controls”, and VA IAM enterprise requirements for both direct and assertion based authentication. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of both Personal Identity Verification (PIV) and Common Access Card (CAC). Assertion authentication at a minimum must include Security Assertion Markup Language (SAML) token authentication and authentication/account binding based on trusted headers. Specific Identity and Access Management PIV requirements are set forth in OMB Memoranda M-04-04 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf), M-05-24 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf), M-11-11 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf), National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, and supporting NIST Special Publications. For applications, software, or hardware that cannot support PIV authentication, a Risk Based Decision must be approved by the Deputy Assistant Secretary for Information Security.

A signed waiver has been obtained from the VA OIT CIO Office that the IPv6 requirement cannot be met, and as a result, IPv6 is not a requirement for this effort.

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directive issued by the Office of Management and Budget (OMB) on September 28, 2010 (https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf) & (http://www.cybertelecom.org/dns/ipv6usg.htm). IPv6 technology, in accordance with the USGv6: A 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, including all internal infrastructure and applications shall communicate using native IPv6 operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services, in addition to OMB/VA memoranda, can be found at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282.

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-

05.pdf), M08-23 mandating Domain Name System Security (NSSEC) (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 (http://www.dhs.gov/sites/default/files/publications/TIC_Ref_Arch_v2%200_2013.pdf).

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 9 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Internet Explorer 11, Office 2013, and Windows 8.1. However, Internet Explorer 11, Office 2013 and Windows 8.1 are not the VA standard yet and are currently not approved for use on the VA Network, but are in-process for future approval by OI&T. Upon the release approval of Internet Explorer 11, Office 2013, and Windows 8.1 individually as the VA standard, Internet Explorer 11, Office 2013, and Windows 8.1 will supersede Internet Explorer 9, Office 2010, and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be delivered as a signed .msi package and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA's current desktop application deployment tool. Signing of the software code shall be through a vendor provided certificate that is trusted by the VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) specific to the particular client operating system being used.

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 OI&T Project Managers and teams to meet their mission: delivering world-class IT products that meet business needs on time and within budget.

The Contractor shall utilize ProPath, the OI&T-wide process management tool that assists in the execution of an IT project (including adherence to PMAS standards). It is a one-stop shop providing critical links to the formal approved processes, artifacts, and templates to assist project teams in facilitating their PMAS-compliant work. ProPath is used to build schedules to meet project requirements, regardless of the development methodology employed.

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 Suitability and Security Program,” Appendix A)
Low / Tier 1	**Tier 1 / National Agency Check with Written Inquiries (NACI)** A Tier 1/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 / Tier 2	**Tier 2 / Moderate Background Investigation (MBI)** A Tier 2/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.
High / Tier 4	**Tier 4 / Background Investigation (BI)** A Tier 4/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	Tier1 / Low / NACI	Tier 2 / Moderate / MBI	Tier 4 / High / BI

5.1	□	X	□
5.2	□	□	□
5.3	□	□	□
5.4	□	□	□
5.5	□	X	□
5.6	□	X	□
5.7	□	□	□
5.8	□	□	□
5.9	□	□	□
5.10	□	□	□
5.11	□	□	□

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 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 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the ProPath template. The Contractor Staff Roster shall contain the Contractor’s Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.

d. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.

e. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:

    1) For a Tier 1/Low Risk designation:
        a) OF-306
        b) DVA Memorandum – Electronic Fingerprints
    2) For Tier 2/Moderate or Tier 4/High Risk designation:
        a) OF-306
        b) VA Form 0710
        c) DVA Memorandum – Electronic Fingerprints

f. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).

g. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via eQIP).

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 loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.

l. Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

Deliverable:

A. Contractor Staff Roster

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**
A. Technical Needs	1. Shows understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Offers quality services/products	Satisfactory or higher
B. Project Milestones and Schedule	1. Quick response capability 2. Products completed, reviewed, delivered in timely manner	Satisfactory or higher

	3. Notifies customer in advance of potential problems	
C. Project Staffing	1. Currency of expertise 2. Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
D. Value Added	1. Provided valuable service to Government 2. 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 VPN, or VA Remote Access Security 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 (additional requirements of the contract consolidated into an addendum for easy reference) refer to **Error! Reference source not found.** Additional VA Requirements, Consolidated and ADDENDUM B - VA Information And Information System Security/Privacy Language