



PERFORMANCE WORK STATEMENT (PWS) DEPARTMENT OF VETERANS AFFAIRS

**Office of Information & Technology
Office of Enterprise Cyber Security**

CDM Optimization and Integration Support (CDMO/I)

May 31, 2017

TAC-17- 44964

PWS Version Number: 1.0

Contents

1.0	BACKGROUND.....	3
2.0	APPLICABLE DOCUMENTS.....	5
3.0	SCOPE OF WORK.....	9
3.1	ORDER TYPE.....	9
4.0	PERFORMANCE DETAILS.....	10
4.1	PERFORMANCE PERIOD.....	10
4.2	PLACE OF PERFORMANCE.....	10
4.3	TRAVEL.....	10
5.0	SPECIFIC TASKS AND DELIVERABLES.....	11
5.1	PROJECT MANAGEMENT.....	11
5.1.1	CONTRACTOR PROJECT MANAGEMENT PLAN (BASE AND OPTIONS)	11
5.1.2	REPORTING REQUIREMENTS (BASE AND OPTIONS).....	11
5.1.3	TECHNICAL KICKOFF MEETING (BASE).....	12
5.2	CMD SOLUTION IMPLEMENTATION AND INTEGRATION SERVICE (Base and Options).....	12
5.3	CDM OPERATIONS AND MAINTENANCE (O&M) SUPPORT (Base and Options).....	13
5.3.1	CDM SENSOR CONFIGURATION AND MAINTENANCE SUPPORT (BASE AND OPTIONS).....	13
5.3.2	RAPID RESPONSE SENSOR MAINTANCE SUPPORT (BASE AND OPTIONS).....	14
5.4	CDM DATA INTEGRATION.....	15
5.4.1	CDM DATA INTEGRATION LAYER MAINTENANCE, CONFIGURATION AND REPORTING SUPPORT (BASE AND OPTIONS).....	15
5.5	CDM DASHBOARD CONFIGURATION AND MAINTENANCE (BASE and Options).....	15
5.6	CDM ONGOING GOVERNANCE AND TRAINING SUPPORT (BASE and OPTIONS).....	16
5.7	FUTURE CDM PLATFORM SUPPORT (OPTION PERIODS).....	16
5.8	CDM TRANSITION SUPPORT.....	19
6.0	GENERAL REQUIREMENTS.....	20
6.1	ENTERPRISE AND IT FRAMEWORK.....	20
6.2	SECURITY AND PRIVACY REQUIREMENTS.....	22
6.2.1	POSITION/TASK RISK DESIGNATION LEVEL(S).....	22
6.2.2	CONTRACTOR PERSONNEL SECURITY REQUIREMENTS.....	23
6.3	METHOD AND DISTRIBUTION OF DELIVERABLES.....	25
6.4	PERFORMANCE METRICS.....	25
6.5	FACILITY/RESOURCE PROVISIONS.....	26
6.6	GOVERNMENT FURNISHED PROPERTY.....	28
	ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED.....	29
	ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE.....	36

1.0 BACKGROUND

The mission of the Department of Veterans Affairs (VA), Office of Information & Technology (OI&T), and the Office of Cyber Security Policy and Compliance (OCSPC) 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 system in an effective, timely and compassionate manner. VA depends on Information Management/Information Technology (IM/IT) systems to meet mission goals.

VA employs nearly 400,000 people worldwide, including those located in Guam, Puerto Rico and the Philippines. VA utilizes a highly decentralized management structure whereby the authority to make decisions is delegated to the lowest management level practical. While this streamlines the decision process for delivering services to the public, it significantly complicates the process for maintaining the security and other administrative controls necessary in today's networked information systems environment. OCSPC is responsible for providing centralized cybersecurity guidance and services to VA by addressing issues that cut across administration lines. These centralized services may impact directly on cyber security or other administrative issues.

The vision of OI&T and OCSPC is to advance VA's overall cybersecurity posture through enhanced visibility and with leading edge guidance, support and tools, while ensuring VA and its mission partners' information systems, practices, policies and procedures comply with Federal mandates. OCSPC has the requirement to support the remediation of security risks in new and legacy application systems and to maintain a comprehensive information security program, which includes compliance oversight, to support the resolution of security related vulnerabilities in VA's major systems.

VA's environment is highly complex and geographically dispersed. The VA is tasked with monitoring more than 4.5 million emails per day, tracking and defending from 55,000 new malware variants per day and safeguarding 750,000 connected network devices. This environment requires automated security and compliance capabilities to not only protect against VA's known threats, vulnerabilities and weaknesses but also to understand information security control compliance as mandated by policy. In response to the need to better manage and defend the network, the VA established the Enterprise Cybersecurity Strategy (ECST). The ECST was designed to align with the Office of Management and Budget's (OMB's) Memorandum M-16-04, Cyber Strategy and Implementation Plan (CSIP) for the Federal Civilian Government and to address many key objectives including:

- Prioritized identification and protection of high value information and assets.
- Timely detection of and rapid response to cyber incidents.
- Rapid recovery from incidents when they occur and accelerated adoption of lessons learned from the (Cyber) Sprint assessment.
- Integrate results for Data Sharing Knowledge Management System.

CDM Optimization and Integration Support (CDMO/I)

TAC Number: TAC-17-44964

- Develop metrics to measure harmonized capabilities against comprehensive National Institute of Standards and Technology (NIST)-based framework.
- Develop feedback loop to automate Enterprise Cybersecurity Architecture to incorporate existing and new technologies.

The ECST addresses these specific objectives and supports fundamental change in the overall VA cyber security capabilities of the VA. The ECST consists of eight cybersecurity domains to address the long-standing Material Weakness in Information Security (i.e. deficiencies).

The Department of Homeland Security (DHS) established the Continuous Diagnostics and Mitigation (CDM) program as a dynamic approach to fortify the government's networks and systems. The program provides participating Federal Agencies with required capabilities to assess information security risks on an ongoing basis and to address continuous monitoring and reporting requirements outlined in OMB Memorandum 14-03. The Department of Veterans Affairs (VA) is part of a 7 Agency group (CDM Task Order (TO) 2B) and is receiving CDM products and services to design, implement and operate the CDM solution and address DHS CDM Phase 1 requirements across the Hardware Asset Management (HWAM), Software Asset Management (SWAM), Configuration Management and Vulnerability Management security domains.

Once VA's O&M contractual obligation has expired, VA will assume the responsibilities for the operations and maintenance (O&M) of the CDM tool suite. The new VA CDM O&M responsibilities will be an addition to the assignments currently distributed throughout the entire VA Information Technology (IT) resources. The successful deployment and integration of the CDM sensors and components at VA represents a significant cybersecurity milestone. However, if the CDM tool solution is not adequately supported, these tools have the potential to introduce severe risks with consequential impact to the VA enterprise network. When any new technology is deployed, the potential risk to the network is amplified as the technical resources improve their familiarity, effectiveness and efficiencies with operating the new tools.

VA's CDM solution is highly complex with a combination of existing legacy systems and new security tools integrated with a single data integration layer and federated dashboard systems. VA's existing legacy systems include: Tenable Security Center, McAfee Application Control, and IBM BigFix and the new security tool is ForeScout CounterACT. Data from these systems is integrated into a single data integration layer that leverages Splunk and feeds data into VA's CDM dashboard systems for security risk scoring, and Federal Dashboard integration. Table 1 below outlines the CDM solution components and provides a mapping to VA's CDM sensor tools and their status – new or legacy system.

Components of VA's CDM solution are at varying stages of implementation and maturity level with respect to configuration, interfaces, and support. Additionally, given the massive size and distribution of the VA organization, many of the CDM tool

implementations are the largest in the Federal government and in some cases the world (e.g., ForeScout, IBM BigFix) pushing the limits of what these tools can support using standard original equipment manufacturer (OEM) configurations. To sustain this complex system and achieve a low risk transition from the current CDM support contractor, VA needs to engage an integrator with in depth understanding and experience with VA's specific CDM solution architecture, design, and configuration – particularly the 250+ system-to-system interfaces within the VA environment (including Federal CDM dashboard integration). Further, the integrator must have proven experience implementing the CDM tools and applying best practices as several of VA's CDM tools may not achieve Full Operating Capability (FOC) before the end the current CDM integrator's period of performance. The integrator must also possess an extensive understanding of the VA environment including organization roles/responsibilities, network topology and configuration, security policies, governance structures, Assessment and Authorization (SA&A) processes, engineering support process and change control procedures. The integrator should also have established and proven CDM-specific operations and maintenance processes, infrastructure, and best practices with hands-on experience sustaining mission critical systems. This includes tiered service desks, CDM specific service catalog, hands-on experience maintaining VA's CDM tools, strong OEM relationships, and familiarity with OEM tool trouble shooting best practices and escalation procedures.

2.0 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement, the Contractor shall comply with the Federal and VA policies include the following, as applicable:

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 Security and Suitability Program," June 4, 2010, <http://www.va.gov/vapubs/>
9. VA Handbook 0710, Personnel Security and Suitability Security Program, May 2, 2016, <http://www.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, "Managing Federal Information as a Strategic Resource," July 28, 2016
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," March 10, 2015
19. VA Handbook 6500.1, "Electronic Media Sanitization," November 03, 2008
20. VA Handbook 6500.2, "Management of Breaches Involving Sensitive Personal Information (SPI)", October, 28, 2015
21. VA Handbook 6500.3, "Assessment, Authorization, And Continuous Monitoring Of VA Information Systems," February 3, 2014
22. Office of Information Security, Authorization Requirements, Standard Operating Procedures, Version 3.6, March 24, 2017
23. VA Handbook 6500.5, "Incorporating Security and Privacy in System Development Lifecycle", March 22, 2010
24. VA Handbook 6500.6, "Contract Security," March 12, 2010
25. VA Handbook 6500.8, "Information System Contingency Planning", April 6, 2011
26. OI&T ProPath Process Methodology (reference process maps at <http://www.va.gov/PROPATH/Maps.asp> and templates at <http://www.va.gov/PROPATH/Templates.asp>)
27. One-VA Technical Reference Model (TRM) (reference at <http://www.va.gov/trm/TRMHomePage.asp>)
28. National Institute Standards and Technology (NIST) Special Publications (SP)
29. VA Directive 6508, "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 15, 2014
30. VA Handbook 6508.1, "Procedures for Privacy Threshold Analysis and Privacy Impact Assessment," July 30, 2015
31. VA Directive 6300, Records and Information Management, February 26, 2009
32. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
33. OMB Memorandum, "Transition to IPv6", September 28, 2010
34. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015
35. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 24, 2014

36. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
37. 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
38. 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
39. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
40. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
41. Federal Information Processing Standards Publication (FIPS) publication 199, Standards For Security Categorization of Federal Information and Information Systems, February 2004
42. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
43. OMB Memorandum M-16-04, Cyber Strategy and Implementation Plan (CSIP) for the Federal Civilian Government, October 30, 2015
44. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
45. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
46. NIST SP 800-137, [Information Security Continuous Monitoring](#), September 2011
47. NIST SP 800-157, Guidelines for Derived PIV Credentials, December 2014
48. NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
49. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
50. 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>)
51. 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>)
52. 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>)
53. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, Department of Homeland Security, October 1, 2013, https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf
54. OMB Memorandum M-08-05, “Implementation of Trusted Internet Connections (TIC), November 20, 2007

55. OMB Memorandum M-08-23, Securing the Federal Government's Domain Name System Infrastructure, August 22, 2008
56. 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>)
57. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
58. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
59. Executive Order 13693, “Planning for Federal Sustainability in the Next Decade”, dated March 19, 2015
60. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
61. VA Directive 0058, “VA Green Purchasing Program”, July 19, 2013
62. Office of Information Security (OIS) VAIQ #7424808 Memorandum, “Remote Access”, January 15, 2014, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
63. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
64. VA Memorandum, “Implementation of Federal Personal Identity Verification (PIV) Credentials for Federal and Contractor Access to VA IT Systems”, (VAIQ# 7614373) July 9, 2015, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
65. VA Memorandum “Mandatory Use of PIV Multifactor Authentication to VA Information System” (VAIQ# 7613595), June 30, 2015, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
66. VA Memorandum “Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges” (VAIQ# 7613597), June 30, 2015; <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
67. Public Law 100-235, Computer Security Act of 1987. Clinger-Cohen Act
68. Office of Management and Budget (OMB) Circular A-123, Management Accountability and Control
69. Presidential Decision Directive (PDD) 63
70. E-Government Act of 2002 (Public Law 107-347)
71. Federal Information Security Control Audit Manual (FISCAM)
72. The Government Paperwork Elimination Act
73. Electronic Signatures in Global and National Commerce Act
74. Systems Development Life Cycle Process Description and Guideline Manual, Veterans Benefits Administration, Department of Veterans Affairs, December 1993
75. IEEE 12207, Standard for Information Technology Software Life Cycle Processes
76. SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations
77. SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories

78. Defense Information Systems Agency (DISA) Application Security and Development Security Technical Implementation Guide (STIG)
79. Institute of Electrical and Electronics Engineers (IEEE) Software Engineering Body of Knowledge
80. Building Security In Maturity Model (BSIMM) Software Security Framework
81. Software Assurance Maturity Model
82. VA Directive 6330, Directives Management, February 26, 2009
83. VA Handbook 6330, Directives Management Procedures, October 21, 1993.
84. "Veteran Focused Integration Process (VIP) Guide 1.0", December, 2015, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>
85. "VIP Release Process Guide", Version 1.4, May 2016, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4411>
86. "POLARIS User Guide", Version 1.2, February 2016, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4412>
87. VA Enterprise Cybersecurity Strategy (ECST)
88. ECST Integrated Master Schedule (IMS)

3.0 SCOPE OF WORK

The scope of work for this effort shall include further support of the implementation tasks and continued, comprehensive sustainment and O&M support for the CDM solution. This shall include the following activities:

- Advancing of remote ForeScout deployment tasks to include but not be limited to integration with the VA's multiple ForeScout Virtual Enterprise Managers, SolarWinds and Splunk; and policy creation and implementation as well as appliance monitoring and performance tuning.
- Executing integration activities within the CDM instance of Splunk to include verifying and administering the required functionality between the remote forwarders, indexers, search heads and sensor tool data sources to include ForeScout, IBM BigFix, Tenable Nessus and McAfee Application Control.
- Performing administration functions including five instances of RSA Archer used for CDM reporting purposes.
- Supporting governance and training activities as they relate to the CDM program.
- Developing transition plans and supporting transition activities to ensure uninterrupted CDM services.

3.1 ORDER TYPE

The effort shall be proposed on a **Firm Fixed Price (FFP)** basis.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The recommended period of performance of this effort is as follows:

- Base Period: September 1, 2017 – April 30, 2018
- Option Period 1: May 1, 2018 – April 30, 2019
- Option Period 2: May 1, 2019 – April 30, 2020
- Option Period 3: May 1, 2020 – April 30, 2021

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

There are 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

Efforts under this task order (TO) shall be performed at the Contractor's facility.

The Contractor staff shall be available to coordinate with VA-OCSPC staff on normal Federal Government workdays and be responsive between the core hours of 8:00am and 5:00pm EST.

4.3 TRAVEL

It is anticipated that travel will be required under this effort to perform the tasks and attend program-related meetings through the period of performance.

The total estimated number of trips in support of this effort is up to 6 trips per contract period to the CRRC in Martinsburg, WV and/or VA Medical or Data Centers that are hosting CDM hardware. These trips shall be three days in duration, requiring a minimum of two (2) travelers each.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the same tasks in the option periods as in the base period.

The Contractor shall perform the following:

5.1 PROJECT MANAGEMENT

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN (BASE AND OPTIONS)

The Contractor shall deliver a Contractor Project Management Plan (CPMP) that lays out the Contractor's approach, timeline and tools to be used in execution of this TO effort. 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 initial baseline CPMP shall be concurred upon and updated in accordance with Section B of the TO. The Contractor shall update and maintain the VA Program Manager (PM) approved CPMP throughout the PoP.

Deliverable:

A. Contractor Project Management Plan

5.1.2 REPORTING REQUIREMENTS (BASE AND OPTIONS)

The Contractor is required to provide the Contracting Officer's Representative (COR) with a Monthly Status Report (MSR). In addition, the Contractor shall attend a monthly teleconference meeting with the VA OCSPC staff to discuss and document any issues, pending deliverables or other pertinent topics concerning the task areas.

During the monthly status meetings, the Contractor shall create meeting minutes utilizing MS Word and include this information in the Monthly Status Report. The Contractor shall ensure the minutes contain notes on all significant discussions. The Contractor shall ensure that a Monthly Status Report is submitted outlining the burn report of expenditures for the T&M portion of the contract documented in Task 5.5, action items, progress, status, and any problems/issues encountered in the performance of this task. The MSR 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 its plan and timeframe for resolving the issue. It is expected that

the Contractor will keep in communication with each of the Directors of the Project Management Offices (PMO) so that as issues arise, they are articulated to all the respective parties to prevent escalation of outstanding issues.

In addition to the monthly status meetings, the Contractor shall also attend a weekly status meeting (may be virtual) to review the current status of each task, as well as daily status calls (Monday through Friday) to review high priority issues.

Deliverable:

A. Monthly Status Report

5.1.3 TECHNICAL KICKOFF MEETING (BASE)

The Contractor shall hold a technical kickoff meeting within 10 days after TO award. The Contractor shall present, for review and approval by the Government, the details of the intended approach, work plan, and project schedule for each effort. The Contractor shall specify dates, locations (can be virtual), agenda (shall be provided to all attendees at least five calendar days prior to the meeting), and meeting minutes (shall be provided to all attendees within three calendar days after the meeting). The Contractor shall invite, at a minimum, the CO, Contract Specialist (CS), COR, and the VA PM.

Deliverables:

- A. Kickoff Meeting Agenda and Presentation
- B. Kickoff Meeting Minutes

5.2 CDM SOLUTION IMPLEMENTATION AND INTEGRATION SERVICE (BASE AND OPTIONS)

Implementation and integration support shall be provided to ensure Full Operational Capability (FOC) of the CDM solution. This effort shall include the following:

- Provide implementation planning support for the deployment of VA's application whitelisting solution. Activities include defining implementation processes, work activities, and plans, and developing implementation architectures and designs, governance processes, and VA software whitelist policies. This will also include integration of best practices and lessons learned from previous CDM-related application whitelisting deployments. This information will be provided in a Design Document.
- Integrate outstanding ForeScout appliances from the CDM Phase 1 period of performance with the VA's multiple ForeScout Virtual Enterprise Managers, SolarWinds and Splunk. Assist with the development of and implement VA-specific desired state policies and configurations, tuning the appliances for optimal performance, trouble-shooting of tier 1, 2 and 3 issues that arise, and monitoring system and interface performance and availability.
- Develop and implement system integrations between VA's CDM sensors and the CDM Data Integration Layer (i.e., Splunk). This activity will include designing,

developing, configuring, tuning, documenting, and testing integrations with ForeScout, Tenable Security Center, McAfee Application Control, and IBM BigFix systems using CDM Data Model. Document system interface specifications with in the Design Document.

- Implement and configure VA's CDM Dashboard system for each of the VA Regions including configuring reports, roles, privileges, workflows and interfaces between the CDM Data Integration Layer system and VA's 5 CDM Dashboard instances. Work with DHS to implement interfaces between the VA CDM Dashboard system and the Federal CDM Dashboard using approved DHS interface specifications, guidance, and Data Model.
- Develop processes, procedures and engineering documentation for operating and maintaining the CDM solution and document in Transition Support Plan. Identify and document roles and responsibilities aligned to O&M processes and procedures. Develop and implement workflows and escalations within the designated VA IT Service Management (ITSM) ticketing system for CDM solution problem, issue, and incident management. Develop and implement change control and configuration management processes and procedures for each component of VA's CDM solution.

Deliverables:

- A. Design Document
- B. Change Control and Configuration Management Standard Operating Procedures (SOP)
- C. Transition Support Plan

5.3 CDM OPERATIONS AND MAINTENANCE (O&M) SUPPORT (BASE AND OPTIONS)

5.3.1 CDM SENSOR CONFIGURATION AND MAINTENANCE SUPPORT (BASE AND OPTIONS)

The contractor as ongoing support for the CDM sensor configuration and maintenance activities will be necessary for the VA's ForeScout CounterACT system. This effort shall include the following, with all actions documented in an O&M Concept of Operations:

- Administer and configure VA's ForeScout system including IP segment management, developing and maintaining reports, monitoring system backups, providing ongoing performance monitoring, tuning, and maintaining technical documentation.
- Configure and maintain ForeScout HWAM desired state policies in accordance with VA governance processes and provide change control support. Develop and provide a Configuration Summary Report.

- Maintain user roles and privileges, manage user access, and perform user on/off-boarding.
- Monitor, tune, troubleshoot, and test ForeScout integrations with VA legacy systems including network devices, directory services, Security Information and Event Management (SIEM) systems, and other VA-specific systems.
- Monitor OEM vendors for new releases and updates; perform planning, analysis, and testing for new releases and upgrades. Perform periodic upgrades for CounterACT Enterprise Manager and CounterACT Appliances in conjunction with VA engineering team.
- Create and maintain a Platform Summary of Changes Report inclusive of version upgrades, database schema changes, and patches.

Deliverables:

- A. O&M Concept of Operations by system application
- B. Configuration Summary Report by system application
- C. Performance and Testing Report by system
- D. Platform Summary of Changes by application

5.3.2 RAPID RESPONSE SENSOR MAINTANCE SUPPORT (BASE AND OPTIONS)

As VA's CDM implementation achieves FOC, systems availability and performance will become critical to ensure VA maintains 100% visibility of IP addressable devices on its networks and reduces the attack surface by quickly removing rogue or unauthorized devices. VA's ForeScout solution is highly distributed with deployments to 250+ locations across the US. Although the ForeScout system is configured for remote management using the Integrated Dell Remote Access Controller (iDRAC) system, in certain cases touch labor is required to support troubleshooting and appliance replacement activities. Many of these VA locations lack technical resources that can quickly respond to ForeScout appliance outages and process defective devices through the OEM's Return Merchandize Authorization (RMA) process. To address this gap and achieve high availability for the VA's ForeScout solution, the effort shall include the following:

- Ability to deploy ForeScout engineers to VA locations within the US within 24-48 hours to support onsite ForeScout system outages, troubleshooting, and appliance replacement activities.
- Coordinate onsite response and support activities with the OEM, VA engineering teams, and site personnel.
- Continue to enhance remote monitoring and configuration activities to minimize travel and increase availability service level targets.

5.4 CDM DATA INTEGRATION

5.4.1 CDM DATA INTEGRATION LAYER MAINTENANCE, CONFIGURATION AND REPORTING SUPPORT (BASE AND OPTIONS)

Maintenance for the data integration layer system will be needed for VA's CDM solution in conjunction with VA's existing Network and Security Operations Center (NSOC) Splunk support team. This effort shall include the following:

- Monitor, maintain, trouble-shoot, and test integrations and interfaces between VA's CDM sensors (e.g., ForeScout, BigFix, Tenable SC, McAfee Application Control) and the Splunk data integration layer.
- Develop and maintain CDM reports and applications.
- Monitor and report on data integration system performance and availability.
- Analyze and support planned OEM product upgrades; provide testing and update engineering documentation such as installation, user and configuration management guides and plans.
- In coordination with the NSOC, support user roles/privileges maintenance and user access control.
- Monitor data quality and provide ongoing quality reporting; perform root cause analysis for data quality issues.
- Provide a Data Model which includes data mapping, configuration, administrative controls and related information associated with the existing data warehouse.

Deliverables:

- A. Data Model (for System Design)

5.5 CDM DASHBOARD CONFIGURATION AND MAINTENANCE (BASE AND OPTIONS)

Contractor shall be provided for ongoing CDM dashboard configuration and maintenance, including the following activities:

- Provide administration and configuration support for each of VA's 5 CDM dashboard instances.
- Develop new and maintain existing CDM dashboard reports.
- Monitor, maintain, and troubleshoot integrations between VA's data integration layer and each CDM Dashboard instance.
- Monitor and maintain integration between VA's CDM Dashboard instances and the DHS Federal Dashboard.
- Maintain user roles and privileges; manage user access and perform user on/off-boarding.

- Coordinate with DHS on new CDM dashboard releases and upgrades; perform planning, analysis, configuration and testing for new releases. Perform CDM Dashboard release upgrades in coordination with VA engineering team.
- Provide a Dashboard Configuration Summary to include configuration information, data flow, data models, passwords links, and data composition.

Deliverables:

A. Dashboard Configuration Summary

5.6 CDM ONGOING GOVERNANCE AND TRAINING SUPPORT (BASE AND OPTIONS)

Contractor will provide ongoing governance and training support will be necessary for VA's CDM Solution. This effort shall include the following:

- Maintain and update CDM change control and configuration management processes and procedures.
- Prepare and submit change request packages for VA Change Advisory Board (CAB) review and approval for CDM solution system change requests.
- Maintain and update VA desired state policies for CDM tools. Coordinate with the DHS CDM governance team on training and lessons learned. Design a CDM O&M Training Plan and training schedule, to include on-line training modules. It is estimated that no more than 4 modules at approximately 1 hour in duration will be required.
- Assist VA with integrating CDM governance processes with existing VA governance structures and initiatives.
- Provide ongoing CDM tool technical, administrative and user training.

Deliverables:

A. CDM O&M Training Plan

5.7 FUTURE CDM PLATFORM SUPPORT (OPTION PERIODS)

The Contractor shall provide technical support services to maintain a future platform of servers and supporting the expansion and optimization of the CDM tools and they are released by DHS in future phases and required to be implemented in the VA environment. This task is meant to allow for the expansion of this contract to support a similar systems within the same logical and physical space and optimally leveraging resources and limiting inter-contract issues should it be required. The expectation would be limited to common technologies found throughout the Federal Government and commercial industry. This task is not expected to be exercised in the base year.

The Contractor shall provide ongoing services as needed to support platform future capacity expansion and hardware/software upgrades during the period of performance.

As updates to hardware and software occur, Contractor expertise is expected to be maintained through an effective continuing education strategy that is in-line with industry standards for the technologies listed within the PWS. Training related to any new technologies can be performed during business hours as long as support coverage for existing systems is maintained.

1. The Contractor shall provide the following technical support tasks:

- a) **Database maintenance:** The Contractor shall provide all typical database (DB) management and administration services such as indexing, table space maintenance, performance tuning, DB layer user management, and database backup planning and execution.
- b) **Application availability:** The Contractor shall ensure a 99% uptime of the Future platform and supporting infrastructure.
- c) **Hardware/software support and problem resolution:** The Contractor shall provide troubleshooting and problem resolution to hardware and software problems. The Contractor shall provide all hardware and software patching and updating services, rack/cable new hardware, and manage firewall and network connections to Hosts (includes patching and performance tuning), replace failed hardware (servers, drives, network cards, etc., assume equipment is under manufacturer's warranty, no cost to Contractor). The Contractor provided support response is expected to be immediate, defined as five (5) minutes or less unless otherwise engaged in an emergency or directed task where this response time is not possible. The Contractor staff shall monitor communication systems continuously to include, phone calls, VA email and VA instant messaging applications during business hours as defined in the PWS. Response for emergencies on off-hours is defined as thirty (30) minutes or less. Critical issues may require escalation to upper management for direction/resolution. All issues will be addressed by Future platform leadership relative to the Future platform supported by the CSHS Team. The Contractor shall work seamlessly with the Future platform team providing full insight into platform configurations (read-only access). The Contractor shall work with the Future Platform Team and pertinent vendor for both the application and hardware to resolve any performance issues with full cooperation and open communication. The single authority going forward will be the Future Platform Team Government leadership.
- d) **Documentation Support.** The Contractor shall be responsible for developing and maintaining a Future Platform EVVM Operational Procedures Summary that describes the processes/procedures needed to completely configure, operate and maintain the environment as determined by the Contractor and confirmed by the Government Program Manager. The Contractor should assume that none exist as these are new platforms and no historical documentation exists.

- e) **Backups.** The Contractor shall provide all database and software backup services, to include database restoration services when specific data sets are requested by appropriate VA.
- f) **Software modifications.** The Contractor shall provide software modification services to support operating systems, virtual machines and databases, to include any which may be necessary for general systems maintenance, such as backups and security configuration maintenance.
- g) **Proactive monitoring.** In-depth, application-level, proactive monitoring shall be performed by the Contractor using the existing CSHS Team established Zenoss server or an alternate tool provided by the Contractor Team. The Contractor shall configure Zenoss infrastructure, database, and application monitoring and provide Zenoss monitoring specifications. The Contractor shall provide the EVVM Team with full read-only access to the Zenoss system and configure automated alerting (e.g. email, SMS, etc.) to the EVVM at their request.
- h) **Storage Area Network (SAN) management.** The Contractor shall administer the SAN (includes patching, monitoring and performance tuning).
- i) **Virtual Machine/VMware management.** The Contractor shall administer VMware ESXi Virtual Hosts (includes patching, monitoring and performance tuning), create new Virtual Machines (VM), install/configure the OS on new VMs, migrate VM within ESXi clusters, manage VM resources as needed, work with and share the ability to Create/Revert/Manage VM snapshots with the Future platform Team as needed. The CSHS Team will be responsible for all VM patching and configuration after initial VM creation.

Future Platform Maintenance and Operations Report. The Contractor shall provide VA Future Platform Maintenance and Operations Report that indicates:

- a. Average uptime for the month.
- b. Historical uptime trending for a sliding twelve (12) month window.
- c. The number of times when any Future platform services, components or systems were unavailable and times of unavailability with hour-based outage summary.
- d. Any patches, changes or updates made and the result of those patches, changes or updates.
- e. Number of database backups performed
- f. The root cause of all performance impacts.

Deliverables:

- A. Future Platform Operational Procedures Summary Plan
- B. Future Platform Maintenance and Operations Report
- C. Future Maintenance and Metrics Dashboards

5.8 CDM TRANSITION SUPPORT

Transitional support will be required if migration to a new support contract is needed. We recommend support to provide Transition Out activities for a period of 60 days, which entails transition support for migrating work from the current contract to a follow-on contract or Government entity. This transition may be to a Government entity or to another Contractor or to the incumbent Contractor under a new contractual vehicle. We recommend a Transition Out Plan for COR/PM review and approval. Coordination with Government staff, successor staff and management, as necessary, will be required. The Transition Out Plan shall also include delivery of copies of all artifacts delivered under this effort, as well as existing policies and procedures, and delivery of baseline metrics and statistics. The report should also include identification of any outstanding CDM O&M issues encountered and any future activities that should be considered as a part of future support. Key issues should be closed out, to include defining performance metrics as the basis of evaluating goal achievement, whether any projects have adequately demonstrated through testing that the system meets its functional and performance requirements and whether the system is adequately supported by documentation, training, etc. All final reports, status updates, and transfer of all appropriate records to the COR shall be accomplished before the period of performance is completed.

Contractor shall conduct analysis, create the strategy, and develop the plans and products needed to successfully transition the provision of services. The Contractor shall:

1. Minimize transition impact to the user community.
2. Ensure no breaks in service availability.
3. Maintain existing service quality and performance levels.
4. Ensure a transparent and seamless transition.
5. Maintain support and meet delivery milestones of ongoing projects.
6. Minimize operations and maintenance (O&M) cost overlaps.
7. Ensure that the IT security posture during transition is maintained at current levels without creating gaps and/or vulnerabilities.
8. Ensure no service disruption or degradation during transition.

The Contractor shall develop and provide a Transition Plan covering transition activities. The Contractor shall then implement the detailed transition strategies and processes needed to enable an efficient transfer of products and services from the incumbent service provider to the service platform without disruption to ongoing contract support levels.

The Contractor shall develop and implement detailed transition strategies and processes needed to maintain continuity of operations and quality of service during the transition period. For planning purposes, the overall transition period shall not exceed sixty (60) days. Transition of operational capabilities is to be completed within sixty (60) days.

The Contractor shall perform the analyses needed to develop the plans for transitioning the contract services and appropriate GFE/GFI to their operational environment as required under this TO and to ensure that all required systems, data, information, domain knowledge, licenses, maintenance contracts, documentation, and other relevant items are identified and transitioned.

The Contractor shall also consider non-personnel issues, such as materials and supplies, equipment, facilities, sub-contracts, leases, environmental issues, safety and security, etc.

At the request of VA OCSPC, the Contractor shall conduct an inventory of GFE and IT assets; establish management processes and controls; and other tasks the Contractor and/or the COR deem necessary to support the transition process.

Deliverable:

A. Transition Out Plan

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.OI&T.va.gov/VA_EA/VAEA_TechnicalArchitecture.asp, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.OI&T.va.gov/enterprise_dp.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, VA Handbook 6500 Appendix F, "VA System Security Controls", and VA IAM enterprise requirements for direct, assertion based authentication, and/or trust based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of Personal Identity Verification (PIV) and/or Common Access Card (CAC), as determined by the business need. Assertion based authentication must include a SAML implementation. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST 800-63 guidelines. Trust based authentication must include authentication/account binding based on trusted HTTP headers. The Contractor solution shall conform to the 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.

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 https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_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 11 and Microsoft Office 2010. In

preparation for the future VA standard configuration update, end user solutions shall also be compatible with Office 2013 and Windows 8.1. However, 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 Office 2013 and Windows 8.1 individually as the VA standard, Office 2013 and Windows 8.1 will supersede 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 IAW the Veteran Focused Integration Process (VIP). VIP is a Lean-Agile framework that services the interest of Veterans through the efficient streamlining of activities that occur within the enterprise. The VIP Guide can be found at <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>. The VIP framework creates an environment delivering more frequent releases through a deeper application of Agile practices. In parallel with a single integrated release process, VIP will increase cross-organizational and business stakeholder engagement, provide greater visibility into projects, increase Agile adoption and institute a predictive delivery cadence. VIP is now the single authoritative process that IT projects must follow to ensure development and delivery of IT products.

The Contractor shall utilize ProPath, the OI&T-wide process management tool that assists in the execution of an IT project (including adherence to VIP 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 VIP compliant work.

6.2 SECURITY AND PRIVACY 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), Federal Bureau of Investigation (FBI) name check, FBI fingerprint check, and written inquiries

Position Sensitivity	Background Investigation (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A)
	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 PWS are:

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low / NACI	Tier 2 / Moderate / MBI	Tier 4 / High / BI
5.1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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) Optional Form 306
 - 2) Self-Certification of Continuous Service
 - 3) VA Form 0710
 - 4) Completed Security and Investigations Center (SIC) Fingerprint Request Form
- 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), 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

ACTION: Review for additional entries. The table below defines the Performance Standards and Acceptable Levels of Performance associated with this effort.

Performance Objective	Performance Standard	Acceptable Levels of Performance
-----------------------	----------------------	----------------------------------

A. Technical / Quality of Product or Service	<ol style="list-style-type: none"> 1. Demonstrates understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Provides quality services/products 	Satisfactory or higher
B. Project Milestones and Schedule	<ol style="list-style-type: none"> 1. Quick response capability 2. Established milestones and project dates are met 3. Products completed, reviewed, delivered in accordance with the established schedule 4. Notifies customer in advance of potential problems 	Satisfactory or higher
C. Project Staffing	<ol style="list-style-type: none"> 1. Currency of expertise and staffing levels appropriate 2. Personnel possess necessary knowledge, skills and abilities to perform tasks 	Satisfactory or higher
D. Management	<ol style="list-style-type: none"> 1. Integration and coordination of all activities to execute effort 	Satisfactory or higher
E. Value Added	<ol style="list-style-type: none"> 1. Provided valuable service to Government 2. Services/products delivered were of desired quality 	Satisfactory or higher

The COR 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 level of performance. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion.

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 may provide remote access to VA specific systems/network in accordance with VA Handbook 6500, which requires the use of a VA approved method to connect external equipment/systems to VA's network. Citrix Access Gateway (CAG) is the current and only VA approved method for remote access users when using or manipulating VA information for official VA Business. VA permits CAG remote access through approved Personally Owned Equipment (POE) and Other Equipment (OE) provided the equipment meets all applicable 6500 Handbook requirements for POE/OE. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved POE or OE. The Contractor shall provide proof to the COR for review and approval that their POE or OE meets the VA Handbook 6500 requirements and VA Handbook 6500.6 Appendix C, herein incorporated as Addendum B, before use. CAG authorized users shall not be permitted to copy, print or save any VA information accessed via CAG at any time. VA prohibits remote access to VA's network from non-North Atlantic Treaty Organization (NATO) countries. The exception to this are countries where VA has approved operations established (e.g. Philippines and South Korea). Exceptions are determined by the COR in coordination with the Information Security Officer (ISO) and Privacy Officer (PO).

This remote access may 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, depending upon the level of access granted. 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 VA Handbook 6500, 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. The Contractor shall ensure all work is performed in countries deemed not to pose a significant security risk. For detailed Security and Privacy Requirements (additional requirements of the contract consolidated into an addendum for easy reference) refer to

6.6 GOVERNMENT FURNISHED PROPERTY

VA will provide access to VA specific systems/network via a Citrix Access Gateway (CAG) as required for execution of tasks performed from Contractor facilities.

DRAFT

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED**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 PM, 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, 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.OI&T.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.

A3.1. 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: <https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards> and <http://www.section508.gov/content/learn/standards>. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

- ☐ § 1194.21 Software applications and operating systems

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

A3.2. Equivalent Facilitation

Alternatively, offerors may propose products and services that provide equivalent facilitation, pursuant to Section 508, subpart A, §1194.5. Such offerors will be considered to have provided equivalent facilitation when the proposed deliverables result in substantially equivalent or greater access to and use of information for those with disabilities.

A3.3. Compatibility with Assistive Technology

The Section 508 standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device. Section 508 requires that the EIT be compatible with such software and devices so that EIT can be accessible to and usable by individuals using assistive technology, including but not limited to screen readers, screen magnifiers, and speech recognition software.

A3.4. Acceptance and Acceptance Testing

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the identified Section 508 standards' requirements for accessibility and must include final test results demonstrating Section 508 compliance.

Deliverables should meet applicable accessibility requirements and should not adversely affect accessibility features of existing EIT technologies. The Government reserves the right to independently test for Section 508 Compliance before delivery. The Contractor shall be able to demonstrate Section 508 Compliance upon delivery.

Automated test tools and manual techniques are used in the VA Section 508 compliance assessment. Additional information concerning tools and resources can be found at <http://www.section508.va.gov/section508/Resources.asp>.

Deliverable:

- A. Final Section 508 Compliance Test Results

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 CO 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 CO 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 CO.
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.

A6.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13693, "Planning for Federal Sustainability in the Next Decade", dated March 19, 2015; Executive Order 13221, "Energy-Efficient Standby Power Devices," dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, Federal Energy Management Program (FEMP) designated, low standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

The Contractor shall ensure that information technology products are procured and/or services are performed with products that meet and/or exceed ENERGY STAR, FEMP designated, low standby power, and EPEAT guidelines. The Contractor shall provide/use products that earn the ENERGY STAR label and meet the ENERGY STAR specifications for energy efficiency. Specifically, the Contractor shall:

1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).
2. Provide/use the purchasing specifications listed for FEMP designated products at https://www4.eere.energy.gov/femp/requirements/laws_and_requirements/energy_star_and_femp_designated_products_procurement_requirements. The Contractor shall use the low standby power products specified at <http://energy.gov/eere/femp/low-standby-power-products>.
3. Provide/use EPEAT registered products as specified at www.epeat.net. At a minimum, the Contractor shall acquire EPEAT® Bronze registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified product lists. The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists.

4. The Contractor shall use these products to the maximum extent possible without jeopardizing the intended end use or detracting from the overall quality delivered to the end user.

The following is a list of information technology products for which ENERGY STAR, FEMP designated, low standby power, and EPEAT registered products are available:

1. Computer Desktops, Laptops, Notebooks, Displays, Monitors, Integrated Desktop Computers, Workstation Desktops, Thin Clients, Disk Drives
2. Imaging Equipment (Printers Copiers, Multi-Function Devices, Scanners, Fax Machines, Digital Duplicators, Mailing Machines)
3. Televisions, Multimedia Projectors

This list is continually evolving, and as a result is not all-inclusive.

ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE

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 (e.g. Business Associate Agreement, Section 3G), 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 CO 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 CO 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 on site 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 CO 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 1600.05, *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 CO 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 CO for response.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require Assessment and Authorization (A&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

1. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*, and the TIC Reference Architecture). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6508, *Implementation of Privacy Threshold Analysis and Privacy Impact Assessment*.

2. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or VA. This includes Internet Explorer 11 configured to operate on Windows 7 and future versions, as required.

3. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default “program files” directory and silently install and uninstall.

4. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

5. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

6. The Contractor/Subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.

7. The Contractor/Subcontractor agrees to:

a. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

i. The Systems of Records (SOR); and

ii. The design, development, or operation work that the Contractor/Subcontractor is to perform;

b. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and

c. Include this Privacy Act clause, including this subparagraph (c), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR.

8. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the Contractor/Subcontractor is considered to be an employee of the agency.

a. "Operation of a System of Records" means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.

b. "Record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person's name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.

c. "System of Records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

9. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as "Systems"), throughout the life of this contract and any extension, warranty, or maintenance periods.

This includes, but is not limited to workarounds, patches, hot fixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploi&Ts of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, based upon the severity of the incident.

11. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes based upon the requirements identified within the contract.

12. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the CO and the VA Assistant Secretary for Office of Information and Technology.

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

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must be in accordance with the TIC Reference Architecture and reviewed and approved by VA prior to implementation.

b. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

c. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires A&A of the Contractor's systems in accordance with VA Handbook 6500.3, *Assessment, Authorization and Continuous Monitoring of VA Information Systems* and/or the VA OCS Certification Program Office. Government-owned (Government facility or Government equipment) Contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

d. The Contractor/Subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA CO and the ISO for entry into the VA POA&M management process. The Contractor/Subcontractor must use the VA POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the Government. Contractor/Subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/Subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the A&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and Contingency Plan). The Certification Program Office can provide guidance on whether a new A&A would be necessary.

e. The Contractor/Subcontractor must conduct an annual self-assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The Government reserves the right to conduct such an assessment using Government personnel or another Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

f. VA prohibits the installation and use of personally-owned or Contractor/Subcontractor owned equipment or software on the VA network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches.

Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

g. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the Contractor/Subcontractor or any person acting on behalf of the Contractor/Subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the Contractors/Subcontractors that contain VA information must be returned to VA for sanitization or destruction or the Contractor/Subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

h. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

- 1) Vendor must accept the system without the drive;
- 2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or
- 3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.
- 4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;
 - a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and
 - b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.
 - c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

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. However, it is the policy of VA to forgo collection of liquidated damages in the event the Contractor provides payment of actual damages in an amount determined to be adequate by the agency.

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 Breaches Involving Sensitive Personal Information*, 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

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the Contractor under the clauses contained within the contract. With 10 working-days' notice, at the request of the Government, the Contractor must fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

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) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* course (TMS #10176) and complete this required privacy and security training annually; Sign and acknowledge (electronically through TMS #10176) 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 any additional cybersecurity or privacy training, as required for VA personnel with equivalent information system access *[to be defined by the VA program official and provided to the CO for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]*

- b. The Contractor shall provide to the CO 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.

CDM Optimization and Integration Support (CDMO/I)
TAC Number: TAC-17-44964

Failure to complete the mandatory annual training and electronically 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.

DRAFT