

PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS

Office of Information & Technology

Enterprise Program Management Office

Enterprise Encryption Key Management System

Date: 8-18-17

**TAC-17-45792**

**PWS Version Number:** 1.0

Contents

[1.0 BACKGROUND 3](#_Toc491698919)

[2.0 APPLICABLE DOCUMENTS 4](#_Toc491698920)

[3.0 SCOPE OF WORK 7](#_Toc491698921)

[4.0 PERFORMANCE DETAILS 7](#_Toc491698922)

[4.1 PERFORMANCE PERIOD 7](#_Toc491698923)

[4.2 PLACE OF PERFORMANCE 8](#_Toc491698924)

[4.3 TRAVEL 8](#_Toc491698925)

[5.0 SPECIFIC TASKS AND DELIVERABLES 9](#_Toc491698926)

[5.1 PROJECT MANAGEMENT 9](#_Toc491698927)

[5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN 9](#_Toc491698928)

[5.1.2 REPORTING REQUIREMENTS 9](#_Toc491698929)

[5.1.3 TECHNICAL KICKOFF MEETING 10](#_Toc491698930)

[5.1.4 RATIONAL TOOLS TRAINING 10](#_Toc491698931)

[5.1.5 PRIVACY & HIPAA TRAINING 11](#_Toc491698932)

[5.2 EEKMS REQUIREMENTS ELABORATION 11](#_Toc491698933)

[5.3 EEKMS System Design and configuration management 12](#_Toc491698934)

[5.4 EEKMS TESTING 12](#_Toc491698935)

[5.5 EEKMS DEPLOYMENT PREPARATION SUPPORT 14](#_Toc491698936)

[5.6 ASSESSMENT AND AUTHORIZATION (A&A) SUPPORT 15](#_Toc491698937)

[5.7 EEKMS INSTALLATION SUPPORT (BASE PERIOD) 16](#_Toc491698938)

[5.8 On-GOING OPERATIONS AND MAINTENANCE SUPPORT (WARRANTY) (BASE PERIOD and OPTION PERIODS) 17](#_Toc491698939)

[5.9 KEY MANAGEMENT INTEGRATION (VISTA READONLY - MSSQL) (BASE PERIOD) 18](#_Toc491698940)

[5.10 KEY MANAGEMENT INTEGRATION (VISTA READ-ONLY – INTERSYSTEM CACHE) (BASE PERIOD) 18](#_Toc491698941)

[5.11 KEY MANAGEMENT INTEGRATION (VISTA PRODUCTION AND DR -INTERSYSTEMS CACHE) (OPTIONAL TASK) 18](#_Toc491698942)

[5.12 KEY MANAGEMENT INTEGRATION (VISTA Data WAREHOUSE – MSSQL, INTERSYSTEMS CACHE) (OPTIONAL TASK) 18](#_Toc491698943)

[5.13 TRANSITION SUPPORT (OPTIONAL FFP TASK) 19](#_Toc491698944)

[6.0 ENTERPRISE AND IT FRAMEWORK 19](#_Toc491698945)

[6.1 SECURITY AND PRIVACY REQUIREMENTS 21](#_Toc491698946)

[6.1.1 POSITION/TASK RISK DESIGNATION LEVEL(S) 22](#_Toc491698947)

[6.1.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS 23](#_Toc491698948)

[6.2 METHOD AND DISTRIBUTION OF DELIVERABLES 25](#_Toc491698949)

[6.3 PERFORMANCE METRICS 25](#_Toc491698950)

[6.4 FACILITY/RESOURCE PROVISIONS 26](#_Toc491698951)

[6.5 GOVERNMENT FURNISHED PROPERTY 27](#_Toc491698952)

[6.6 SHIPMENT OF HARDWARE OR EQUIPMENT 27](#_Toc491698953)

[ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED 29](#_Toc491698954)

[ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE 36](#_Toc491698955)

# BACKGROUND

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

VA operates Veterans Information System and Technology Architecture (VistA), a fully integrated system comprising 181 clinical, financial, and administrative applications integrated within a single database, such that there is only one single authoritative version of any data that all applications use. The VistA database is the Congressionally-mandated single source of truth for Veteran information, and is required to be accessible and usable for the lifetime of the Veteran. The clinical component of VistA (analogous to an Electronic Health Record (EHR)) represents only 50% of VistA’s functionality.

VA is required by Federal laws such as Health Information Portability and Accountability Act (HIPAA) to protect veterans’ information from unauthorized disclosure. One method VA uses to protect information is data encryption. Encryption is used to protect “data at rest” stored in various technologies including physical disk drives, databases and removable media. Encryption is also used to protect data being transmitted between systems using Secure Sockets Layer (SSL).

While many encryption technologies are used by VA, all technologies use a code to encode and decode the data. Managing this code – commonly referred to as a key – is critical to securing encrypted data. Managing keys is time consuming. Keys must be created and securely distributed to a large number of systems. They must be stored and retrieved securely for data recovery in the event of a disaster or system failure. Keys – like passwords - should also be changed regularly. To make this task tractable, short cuts are sometime taken increasing the risk that keys may be compromised.

VA is seeking Contractor solution of products and services for design, implementation and support services of a Commercial-Off-The-Shelf (COTS) Enterprise Encryption Key Management System (EEKMS) to create a uniform, consistent, secure and scalable environment for managing encryption keys and protecting Veterans’ data that conforms to VA policies, Federal regulations and standards. The Contractor shall design and deploy the COTS EEKMS platform and then integrate that platform with specified VA technologies as denoted herein.

While the EEKMS is intended to support the Enterprise VA, initial deployment will be focused on VistA. All VistA support will leverage target technology encryption solutions that support Public-Cryptography Key Standards (PCKS) #11 and/or Key Management Interoperability Protocol (KMIP). This includes, but is not limited to:

|  |  |  |  |
| --- | --- | --- | --- |
| Function | Target Technology | Target Count | Location |
| Vista Production | Intersystems Cache on Linux OS | 260 (130 HA clusters) | Distributed across 6 Data Centers |
| VistA Disaster Recovery | Intersystems Cache on Linux OS | 260 (130 HA clusters) | Distributed across 6 Data Centers |
| Vista Read Only | Intersystems Cache on Linux OS | 130 | 1 in each VA Medical Center |
| VistA Read Only | Mircosoft Sequel Server (MSSQL) on Windows Server | 130 | 1 in each VA Medical Center (VAMC) |
| VistA Data Warehouse | Intersystems Cache on Linux OS | 130 | Distributed across 6 Data Centers |
| VistA Data Warehouse | MSSQL on Windows Server | 130 | Distributed across 6 Data Centers |

The EEKMS will be used by system managers of the managed technology. There are currently 100-200 system managers for VistA.

Below is the release schedule for the EEKMS installations and integration deployments.

|  |  |
| --- | --- |
| **Effort** | **Delivery Date** |
| Austin, TX EEKMS Installing | 90 days from award |
| St. Louis, MO EEKMS Installation | 150 days from award |
| Philadelphia, PA EEKMS Installation | 150 days from award |
| Sacramento, CA EEKMS Installation | 150 days from award |
| EEKMS VistA ReadOnly – MSSQL Integration | 210 days from award |
| EEKMS VistA ReadOnly –Intersystems Cache Integration | 210 days from award |
| EEKMS VistA Production/ DR – Intersystems Cache Integration | 90 days from option exercise |
| EEKMS VistA Data Warehouse –MSSQL / Intersystems Cache Integration | 90 days from option exercise |

# APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement, the Contractor shall comply with the following:

1. Key Management System Baseline Requirements Version 1.7 – August 25, 2017
2. 44 U.S.C. § 3541, “Federal Information Security Management Act (FISMA) of 2002”
3. Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements For Cryptographic Modules”
4. FIPS Pub 201-2, “Personal Identity Verification of Federal Employees and Contractors,” August 2013
5. 10 U.S.C. § 2224, "Defense Information Assurance Program"
6. 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
7. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
8. 42 U.S.C. § 2000d “Title VI of the Civil Rights Act of 1964”
9. VA Directive 0710, “Personnel Security and Suitability Program,” June 4, 2010, <http://www.va.gov/vapubs/>
10. VA Handbook 0710, Personnel Security and Suitability Security Program, May 2, 2016, [http://www.va.gov/vapubs](http://www.va.gov/vapubs" \o "VA Publications Homepage)
11. VA Directive and Handbook 6102, “Internet/Intranet Services,” July 15, 2008
12. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
13. Office of Management and Budget (OMB) Circular A-130, “Managing Federal Information as a Strategic Resource,” July 28, 2016
14. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
15. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
16. 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
17. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
18. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, 2012
19. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” March 10, 2015
20. VA Handbook 6500.1, “Electronic Media Sanitization,” November 03, 2008
21. VA Handbook 6500.2, “Management of Breaches Involving Sensitive Personal Information (SPI)”, October, 28, 2015
22. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring Of VA Information Systems,” February 3, 2014
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. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
42. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
43. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
44. NIST SP 800-157, Guidelines for Derived PIV Credentials, December 2014
45. NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
46. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
47. 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>)
48. 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>)
49. 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>)
50. 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>
51. OMB Memorandum M-08-05, “Implementation of Trusted Internet Connections (TIC), November 20, 2007
52. OMB Memorandum M-08-23, Securing the Federal Government’s Domain Name System Infrastructure, August 22, 2008
53. 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>)
54. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
55. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
56. Executive Order 13693, “Planning for Federal Sustainability in the Next Decade”, dated March 19, 2015
57. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
58. VA Directive 0058, “VA Green Purchasing Program”, July 19, 2013
59. VA Handbook 0058, “VA Green Purchasing Program”, July 19, 2013
60. Office of Information Security (OIS) VAIQ #7424808 Memorandum, “Remote Access”, January 15, 2014, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28>
61. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
62. 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>
63. 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>
64. 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>
65. “Veteran Focused Integration Process (VIP) Guide 1.0”, December, 2015, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>
66. “VIP Release Process Guide”, Version 1.4, May 2016, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4411>
67. “POLARIS User Guide”, Version 1.2, February 2016, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4412>
68. VA Rational Tools Guide <http://vaww.oed.portal.va.gov/communities/OSCTM/toolsmgmt/Rational%20Tools/Documents/Forms/AllItems.aspx>

# SCOPE OF WORK

The Contractor shall provide project management, design, integration, configuration, testing, deployment and support of a COTS Enterprise Encryption Key Management System. The Contractor shall deploy, integrate, and maintain the EEKMS with various encryption technologies in use at VA such that the EEKMS manages the keys for those technologies.

# PERFORMANCE DETAILS

## PERFORMANCE PERIOD

The Period of Performance shall be one year from the date of award with two, 1-year options and optional tasks as described herein.

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

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

Under current definitions, four are set by date:

New Year's Day January 1

Independence Day July 4

Veterans Day November 11

Christmas Day December 25

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

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

Martin Luther King's Birthday Third Monday in January

Washington's Birthday Third Monday in February

Memorial Day Last Monday in May

Labor Day First Monday in September

Columbus Day Second Monday in October

Thanksgiving Fourth Thursday in November

## PLACE OF PERFORMANCE

All tasks, except Task 5.5, under this PWS shall be performed at Contractor facilities. The Contractor shall identify the Contractor’s place of performance in their Task Execution Plan submission. Task 5.5 shall be performed at VA Data Centers (list in Task 4.3 below).

## TRAVEL

The Government anticipates travel under this effort to perform the tasks associated with the effort. Include all estimated travel costs in your firm-fixed price line items. These costs will not be directly reimbursed by the Government.

The total estimated number of trips in support of this effort is four (4) as described in the table below and are only required within the base period.  Anticipated locations include the following, estimated at five (5) days in duration:

|  |  |  |  |
| --- | --- | --- | --- |
| **Destination** | **Duration** | **# of people** | **Purpose** |
| Austin, TX | 5 Days | 2 | Test System Installation |
| Sacramento, CA | 5 days | 2 | System Installation |
| St. Louis, MO | 5 days | 2 | System Installation |
| Philadelphia, PA | 5 days | 2 | System Installation |

# SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

## PROJECT MANAGEMENT

### CONTRACTOR PROJECT MANAGEMENT PLAN

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 the contract.  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 contract. The Contractor shall update and maintain the VA PM approved CPMP throughout the PoP.

**Deliverable**:

1. Contractor Project Management Plan

### REPORTING REQUIREMENTS

The Contractor shall use the VA’s implementation of the Rational Toolset to provide a single Agile project/product lifecycle management tool to track execution details. The Rational Project/Product Data and Artifact Repository will be used to provide a single authoritative project and product data and artifact repository. All OI&T project data and artifacts will be required to be managed in this data and artifact repository daily. All checked out artifacts shall be checked back in daily and any data updated daily. Rational synchronizes all changed information immediately for all team members to access work proficiently without the concern of working on aged information.

The Contractor shall use VA Rational tools in accordance with the VA Rational Tools Guide (reference in Applicable Documents above) to:

1. Input and manage scheduled project/product sprints and backlog
2. Input and manage project/product agile requirements
3. Input and manage project/product risks and issues
4. Input and manage project/product configurations and changes
5. Input and manage project/product test plans and execution
6. Input and manage project/product planning and engineering documentation
7. Input and manage linkages to correlate:
   * 1. requirements to change orders
     2. requirements to configurable items
     3. requirements to risks, impediments, and issues
     4. requirements to test cases and test results to show full traceability.

The Contractor shall show all Agile requirements, changes, tests performed and test results in Rational to show evidence of code coverage and test coverage to all the requirements specified herein. The Contractor shall extract bi-weekly reporting data indicating progress performance against items 1 – 7 herein to provide a bi-weekly Rational-extracted report. This Contractor’s report shall provide VA confirmation that all project components are fully documented and incrementally revised, as evidenced by data in the Rational tool suite. Finally, the Contractor’s report shall provide visibility to the linkages indicating requirements traceability with corresponding test cases and test results, and which demonstrate successful performance indicative of expected results in a production environment.

Deliverable:

1. Bi-weekly (every 2 weeks) Progress Report

### TECHNICAL KICKOFF MEETING

The Contractor shall hold a technical kickoff meeting within 10 days after contract 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 (5) calendar days prior to the meeting), and meeting minutes (shall be provided to all attendees within three (3) calendar days after the meeting). The Contractor shall invite the Contracting Officer (CO), Contract Specialist (CS), COR, and the VA PM.

### RATIONAL TOOLS TRAINING

The Contractor shall complete all of the following VA TMS training courses during the onboarding phase, per PWS 5.2:

1. TMS ID 3878248 - IBM Rational Team Concert - Agile Sprint, Configuration/Change Management Level 1
2. TMS ID 3878249 - IBM Rational Team Concert - Agile Sprint, Configuration /Change Management Level 2
3. TMS ID 3878250 - IBM Rational DOORS Next Generation - Requirements Management Level 1
4. TMS ID 3897036 - IBM Rational DOORS Next Generation - Requirements Management Level 2
5. TMS ID 3897034 - IBM Rational Quality Manager - Quality Management Level 1
6. TMS ID 3897035 - IBM Rational Quality Manager - Quality Management Level 2

Contractor and subcontractor personnel who have completed these VA training courses within the past 24 months and have furnished certificates will not be required to re-take the training courses.

**Deliverables:**

1. Rational Training Certificates

### PRIVACY & HIPAA TRAINING

The Contractor shall submit TMS training certificates of completion for VA Privacy and Information Security Awareness and Rules of Behavior and Health Insurance Portability and Accountability Act (HIPAA) training, and provide signed copies of the Contractor Rules of Behavior in accordance with Section 9, Training, from Appendix C of the VA Handbook 6500.6, “Contract Security.”

**Deliverables:**

1. VA Privacy and Information Security Awareness and Rules of Behavior Training Certificate
2. Signed Contractor Rules of Behavior
3. VA HIPAA Certificate of Completion

## EEKMS REQUIREMENTS ELABORATION

The Contractor shall perform requirements elaboration in conjunction with the VA to analyze and elaborate requirements provided in KMS\_Requirements\_Final v1.7 titled KSM\_Requirements\_Final v1.7. The Contractor shall create and populate an EEKMS backlog identifying all features the team considers relevant to configuring the EEKMS product and for each of the specific integrations defined in Task 5.9-5.12 below. The backlog serves as the primary source for all program requirements and user stories, and the Contractor shall work with the VA team to prioritize the contents.

The Contractor shall develop Epics and User Stories for EEKMS business process, technical, functional and system requirements.

Deliverables:

1. EEKMS Project Backlog

## **EEKMS System Design and configuration management**

The Contractor shall develop an EEKMS System Design Document (SDD) that describes the COTS EEKMS system architecture and integration with the VA infrastructure including each of the integrations defined below in Tasks 5.9 and 5.10 and Tasks 5.11 - 5.12 if exercised. The SDD shall address all of the requirements identified in KMS\_Requirements\_Final v1.7 titled KSM\_Requirements\_Final v1.7 as well as in the project baseline and backlog including all requirements that address reliability, performance, availability, distributed key management and disaster recovery.

The Contractor shall conduct design reviews with the project team and obtain VA approval for the system design.

The Contractor shall also perform configuration management services including:

1. Identify the standard and unique aspects of configuration management to be performed which meets project requirements.
2. Identify types of configuration items pertaining to each product to be placed under configuration management.
3. Create and maintain the Configuration Management (CM) Plan and specify how electronic artifact configuration and version management will be managed. The Contractor shall use VA PM approved tools to manage change, activity, issue, action, risk, and other project data as prescribed by VA standards and processes. VA PM or designee shall approve the Configuration Management Plan.
4. Establish and maintain status reporting on change and configuration management activity, and ensure data records and artifacts are filed and updated daily.

Deliverables:

1. System Design Document
2. Configuration Management Plan

## **EEKMS TESTING**

The Contractor shall perform all testing required to ensure that the requirements identified in KMS\_Requirements\_Final v1.7and the EEKMS Backlog as successfully completed. The Contractor shall conduct testing using industry best practices and One-VA TRM approved tools. The Contractor shall conduct testing related to non-functional requirements (e.g. load, performance, installation, back-out, and rollback). The Contractor shall notify the VA at least three days prior to the start of system tests so that VA can observe the testing if desired.

The Contractor shall develop and deliver a Master Test Plan to indicate the methods, tools, and specific tests and to identify environment ownership and support needs. The Master Test Plan shall indicate the methods by which testing shall be conducted to meet the requirements detailed with this EEKMS Backlog. The Contractor shall also document how test results will be validated by the Government. The Contractor shall perform testing as necessary throughout all lifecycle phases of this contract. The Contractor shall provide the Master Test Plan and associated data in Rational Quality Manager following the templates and data requirements appropriate for each test purpose. The Contractor shall provide test results in Rational Quality Manager which is the final piece of data that completes the RTM. COR and VA PM acceptance will occur through the Rational Quality Manager approval process.

The Contractor shall manage, track and remediate findings and defects from all associated tests. Any vulnerability scans, remediation and reports shall be completed prior to the PM/COR acceptance testing. The Contractor shall perform demonstrations to indicate that the new interfaces perform as designed in accordance with system requirements.

The Contractor shall install and configure the EEKMS system in a Government supplied test environment located in Austin, TX.

The Contractor shall conduct or assist the Government in conducting security scans, accessibility reviews, performance tests, technical standards review, architectural compliance assessments, user acceptance reviews and initial operational capability tests, audits, and reviews. Accessibility reviews are performed through a variety of tool- based and manual reviews, able to scan web applications and other technologies used for user interfaces. Performance testing is done through load testing and technical analysis of capacity planning data submitted by the project team. Architectural compliance assessments are done through submission of design materials to confirm compliance with the approved enterprise architecture.

The Contractor shall ensure all tests, compliance review planning, execution details and their testing and compliance results are entered and maintained in Rational Quality Manager and under version control in Rational Team Concert. Specifically, Test Management Data and Artifacts include such items as cases/scripts, configurations, utilities, tools, plans and results. The Contractor shall ensure that results of all assessments of the project performed by the Contractor are consolidated into Rational for planning and status reporting.

When a defect is identified during testing, the Contractor shall log it in Rational to establish a Defect Listing, selecting the appropriate severity level. The Contractor shall support the Project Manager in prioritizing the defects within the EEKMS backlog by participating in the Defect Management Board (DMB). Based on prioritization the defect could be entered into the current sprint and/or entered into the EKMS backlog.

The Contractor shall ensure the Rational tool data is up-to-date on a daily basis so that VA stakeholders can access accurate and timely status.

The Contractor shall support deployment in the Pre-Production and production environments. VA shall provide metadata from production clones for testing.

**Deliverable:**

1. Master Test Plan
2. Post Development Test Scripts
3. Test Management Data and Artifacts
4. Defect Listing

## **EEKMS DEPLOYMENT PREPARATION SUPPORT**

The VIP Release Process is conducted by one or more assigned Release Agents, who perform frequent, regular reviews of required and appropriately linked product data in the mandated repositories. The Release Agents also provide timely feedback to the product team concerning the status of the product data and the status of the team’s compliance with the VIP Release Process. The Contractor shall support OI&T’s single VIP Release process for the EEKMS.

The POLARIS calendaring process and tool will be used to track software installations, hardware replacements, system upgrades, patch release and implementation, special works in progress, and other deployment events in the VA production environment. The Contractor shall provide data for populating and updating the POLARIS calendaring process for each release and deployment of the EEKMS.

Effective Enterprise Encryption Key management requires consistent implementation of key management methods. The Contractor shall develop a VA Enterprise Encryption Key Management Operations Manual to guide implementation of key management across encryption target technologies.

The Contractor shall ensure the Enterprise Encryption Key Management Operations manual is consistent with all relevant VA policies and standards as defined in the Applicable Documents above. The Contractor shall work with the project team to ensure the Operations Manual is consistent with project requirements and addresses key management issues not addressed by VA policies.

The Contractor shall ensure the Enterprise Encryption Key Management Operations Manual defines VA EEKMS management policies and standards. The Contractor shall update the EEKMS Operations Manual, if required, for each system or application integration. Additionally, the Contractor shall define implementation, management and compliance procedures to ensure that EEKMS is compliant with VA and EEKMS policies and standards. Further, the Operations Manual shall include regular maintenance and operations information, Responsibility, Accountability, Consulted, and Informed (RACI) information, process flowcharts, dataflow diagrams, key monitoring indicators, and troubleshooting information.

The Contractor shall develop a Deployment and Installation Guide which includes back-out and rollback procedures as required by VIP in accordance with the template provided in the ProPath Artifacts Library. The Contractor shall update the Deployment and Installation Guide as necessary.

The Contractor shall develop an Administrator User Manual which addresses procedural information for daily operational use of the software. The Contractor shall update the Administrator User Manual as necessary.

The Contractor shall provide a Computer Based Training (CBT) module for EEKMS administration and configuration to be delivered via the VA Talent Management System. The Contractor shall update the CBT module as necessary.

Upon successful completion of acceptance testing, the Contractor shall notify the Release team, the Portfolio Manager, Business/Product Owner and Receiving Organization to approve the release for further implementation.

The Contractor shall hold test site calls with VA staff to include Release Coordinators and VIP Release Agents once the product is released for production testing.

Deliverables:

1. Enterprise Encryption Key Management Operations Manual
2. Deployment and Installation Guide
3. User Manual
4. Computer Based Training Module

## ASSESSMENT AND AUTHORIZATION (A&A) SUPPORT

The Contractor shall provide support to VA to obtain all required ATOs for this effort. That support shall include providing applicable documentation and coordination with data center partners to ensure consistency with VA ATO requirements for certification. The Contractor shall provide support to demonstrate the EEKMS meets VA information security policies and standards to facilitate the successful completion of the A&A process to obtain an ATO and maintain all managed technology ATOs.

The Contractor shall:

1. Support Field Security Services (FSS) Information Security Officers (ISOs) and Office of Cyber Security (OCS) Security Control Assessment (SCA) team for VistA assessment requirements as detailed in VA Directive and Handbook 6500 Information Security Program, VA Handbook 6500.3 Certification and Accreditation of VA Information Systems.
2. Identify, document, review, and maintain the EEKMS A&A Artifacts as needed to support ATO requests in accordance with VA policy and Federal Law and guidelines, as detailed in NIST SP 800-37 Revision 1 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Additionally, the Contractor shall update any system aspect (e.g. documentation, configuration, etc.) based on comments from the A&A review process conducted.
3. Provide continued security Plan of Actions and Milestones (POAM) support.
4. Perform regular scanning of software code for latent software defects and security vulnerabilities/weaknesses, through a process known as Software Code Quality Checking (SCQC). The purpose of SCQC is to ensure delivery of secure, quality software code, clean code (e.g. free of fragments and dead code), benchmarked against recognized standards. The process focuses on the technical correctness of the code as well as freedom from security vulnerabilities. Software reliability and maintainability, along with a number of other factors, are measured throughout the entire system development life cycle (SDLC) through the use of SCQC tools. The Contractor shall document results in a Certified Scan Report.
5. Provide evidence of having conducted a static code analysis, static security analysis and architectural analysis. The evidence should identify the processes and tools used, to include the use of external independent evaluators, together with the results of the scans. For legacy products, the government will provide to the contractor an SCQC “baseline” of “inherited” technical defects and security vulnerabilities along with the estimated level of effort required to correct the code. Contractors should ensure no new technical flaws or security vulnerabilities are introduced during the correction or enhancement of the code. The Contractor shall document results in the Certified Scan Report.

A&A Artifacts include the following:

1. System Security Plan
2. Security Configuration Plan
3. Information System Contingency Plan (coordinate with Office of Business Continuity)
4. Incident Response Plan
5. Privacy Impact Assessment (coordinate with Office of Privacy)
6. Risk Assessment (coordinate with Office of Risk Management and Incident Reporting)
7. Security Configuration Checklist (SCC)
8. System Interconnection Agreements (MOU and Interconnection)
9. Interconnection Security Agreement
10. Signatory Authority

**Deliverables:**

1. Certified Scan Report
2. A&A Artifacts

## EEKMS INSTALLATION SUPPORT (BASE PERIOD)

The Contractor shall install the EEKMS system in VA Data Centers as directed by VA Project Manager. In performing this task, the Contractor shall:

* Coordinate with VA Contacts at three (3) data centers (Philadelphia, PA, Sacramento, CA, St. Louis, MO) as identified by project manager to ensure required resources are available to successfully deploy EEKMS.
* Schedule installation with VA Data Center Contacts.
* Deliver equipment and software to VA Data Centers in advance of installation.
* Assist VA Data Center staff with physical installation, network connectivity and configuration of HSMs.
* Assist VA Data Center staff with installation and configuration of EEKMS.
* Perform installation tests as defined by test plan (defined in the above section) and record results in Rational.

The Contractor shall provide a Deployment/Installation Checklist that identifies that all of the above tasks were completed successfully.

**Deliverable**:

1. Deployment/Installation Checklist

## On-GOING OPERATIONS AND MAINTENANCE SUPPORT (BASE PERIOD and OPTION PERIODS)

The Contractor shall extend its commercial warranty for all hardware and software acquired as part of this contract.

The Contractor shall provide operational support for the EEKMS as well as all integrations deployed as part of this effort. The Contractor shall provide installation, administration, maintenance and troubleshooting support. The Contractor shall provide maintenance support to include preventive maintenance and scheduled maintenance, and other activities to retain or restore the solution. The Contractor shall also develop and maintain a current library of all operational documentation including logs of operational events, maintenance of operational monitoring and management tools, operational scripts and operational procedures, all to be made available in real time to VA personnel.

The Contractor shall support the VA in resolving defects/issues associated with EEKMS and all integrations. Defects/issues may be identified by the Contractor as part of this task, defects may also be identified by the Government, National Service Desk (NSD), Business/Product Owners and their designees, as communicated by the COR. This support shall include assisting in troubleshooting issues and identifying and coordinating issue resolution. For each defect identified, the Contractor shall triage the defect, identify a resolution for the defect, and provide a plan for resolution, including timeline and impacts to the code and updates to Rational. The Contractor shall deliver Monthly Post Deployment Support Report and Monthly Defect Resolution Plan. Following COR approval of the Contractor defect resolution plan, the Contractor shall execute the approved plan.

Contractor shall also support the VA in planning, testing and deploying system upgrades. All upgrades activities shall be documented in Rationale as required by VA policies and procedures.

**Deliverables:**

1. Monthly Post Deployment Support Report
2. Monthly Defect/Issue Resolution Plan

## KEY MANAGEMENT INTEGRATION (VISTA READONLY - MSSQL) (BASE PERIOD)

The Contractor shall configure the EEKMS to manage the keys for the VistA Read-only MMSQL at VAMCs in accordance with KMS\_Requirements\_Final v1.7 and the EEKMS Backlog. This shall require the Contractor to configure both the EEKMS as well as the integrated system to ensure all of the requirements are met.

The Contractor shall perform all tasks defined in Task 5.2 through 5.8 in execution of this integration.

## KEY MANAGEMENT INTEGRATION (VISTA READ-ONLY – INTERSYSTEM CACHE) (BASE PERIOD)

The Contractor shall configure the EEKMS to manage the keys for Intersystems Cache on VistA Read-only Systems at VAMCs in accordance with KMS\_Requirements\_Final v1.7 and the EEKMS Backlog. This shall require the Contractor to configure both the EEKMS as well as the integrated system MMSQL to ensure all of the requirements are met.

The Contractor shall perform all tasks defined in Task 5.2 through 5.8 in execution of this integration.

## KEY MANAGEMENT INTEGRATION (VISTA PRODUCTION AND DR -INTERSYSTEMS CACHE) (OPTIONAL TASK)

The Contractor shall configure the EEKMS to manage the keys for Vista Production and Disaster Recovery Systems – Intersystems Cache in accordance with KMS\_Requirements\_Final v1.7and the EEKMS Backlog. This shall require the Contractor to configure both the EEKMS as well as the integrated system to ensure all of the requirements are met.

The Contractor shall perform all tasks defined in Task 5.2 through 5.8 in execution of this integration.

## KEY MANAGEMENT INTEGRATION (VISTA Data WAREHOUSE – MSSQL, INTERSYSTEMS CACHE) (OPTIONAL TASK)

The Contractor shall configure the EEKMS to manage the keys for Vista Data Warehouse – MSSQL, Intersystems Cache in accordance with KMS\_Requirements\_Final v1.7 and the EEKMS Backlog. This shall require the Contractor to configure both the EEKMS as well as the integrated system to ensure all of the requirements are met.

The Contractor shall perform all tasks defined in Task 5.2 through 5.8 in execution of this integration.

## TRANSITION SUPPORT (OPTIONAL FFP TASK)

The Contractor shall provide a plan for 60 days of outgoing transition support upon the approval of the Transition Plan for transitioning work from the current task order to a follow-on task order or Government entity.  This transition may be to a Government entity or to another Contractor.  Additionally, in accordance with the Government-approved plan, the Contractor shall assist the Government in planning and execution/implementation of the complete transition from this contract to another entity.  This shall include formal coordination with Government staff and successor staff and management.  It shall also include delivery of copies of existing policies and procedures, and delivery of required metrics and statistics. The Transition Plan shall include, but is not limited to:

1. Coordination with Government representatives
2. Review, evaluation and transition of current support services
3. Transition of historic data to new Contractor system
4. Transition of Rational accounts
5. Transfer of hardware and software warranties, maintenance agreements and licenses
6. Transfer of all necessary business and/or technical documentation
7. Orientation phase and program to introduce Government and Contractor personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes
8. Disposition of Contractor purchased Government owned assets,
9. Transfer of Government Furnished Equipment (GFE) and Government Furnished Information, and GFE inventory management assistance
10. Turn-in of all Government keys, ID/access cards, and security codes

**Deliverable**:

1. Transition Plan

# ENTERPRISE AND IT FRAMEWORK

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

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are PIV-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), <http://www.ea.oit.va.gov/VA_EA/VAEA_TechnicalArchitecture.asp>, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, <http://www.techstrategies.oit.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.

## SECURITY AND PRIVACY REQUIREMENTS

### 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 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 |  |  |  |
| 5.2 |  |  |  |
| 5.3 |  |  |  |
| 5.4 |  |  |  |
| 5.5 |  |  |  |
| 5.6 |  |  |  |
| 5.7 |  |  |  |
| 5.8 |  |  |  |
| 5.9 |  |  |  |
| 5.10 |  |  |  |

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

### CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

**Contractor Responsibilities:**

1. 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.
2. The Contractor shall bear the expense of obtaining background investigations.
3. 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.
4. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
5. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
6. Optional Form 306
7. Self-Certification of Continuous Service
8. VA Form 0710
9. Completed Security and Investigations Center (SIC) Fingerprint Request Form
10. 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).
11. 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).
12. 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.
13. 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).
14. 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.
15. 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.
16. 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:**

1. Contractor Staff Roster

## 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).

## PERFORMANCE METRICS

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

| **Performance Objective** | **Performance Standard** | **Acceptable Levels of Performance** |
| --- | --- | --- |
| 1. Technical / Quality of Product or Service | 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 |
| 1. Project Milestones and Schedule | 1. Established milestones and project dates are met 2. Products completed, reviewed, delivered in accordance with the established schedule 3. Notifies customer in advance of potential problems | Satisfactory or higher |
| 1. Cost & Staffing | 1. Currency of expertise and staffing levels appropriate 2. Personnel possess necessary knowledge, skills and abilities to perform tasks | Satisfactory or higher |
| 1. Management | 1. Integration and coordination of all activities to execute effort | 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.

## 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 ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED and ADDENDUM B - VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE.

## GOVERNMENT FURNISHED PROPERTY

The Government will not provide IT accessories including but not limited to Mobile Wi-Fi hotspots/wireless access points, additional or specialized keyboards or mice, laptop bags, extra charging cables, extra PIV readers, peripheral devices, additional RAM, etc. The Contractor is responsible for providing these types of IT accessories in support of the contract as necessary and any VA installation required for these IT accessories shall be coordinated with the COR.

## SHIPMENT OF HARDWARE OR EQUIPMENT

**Inspection:** Destination  
**Acceptance:** Destination  
**Free on Board (FOB):** Destination

**Ship To and Mark For:**

|  | Primary |  | Alternate |
| --- | --- | --- | --- |
| Name: |  | Name: |  |
| Address: |  | Address: |  |
| Voice: |  | Voice: |  |
| Email: |  | Email: |  |

Special Shipping Instructions:

The Contractor shall complete the Master Delivery Schedule in accordance with the Instructions, and shall coordinate with the COR for specifics. The Master Delivery Schedule shall be provided after award and updated prior to and after each delivery timeframe.

Shipment/Delivery Kick-off Meeting

The Contractor shall conduct a Shipment/Delivery Kick-off Meeting with the VA PM, COR, Delivery Date Coordinator, Implementation Manager, and Facility CIOs (or designee) to discuss delivery schedule requirements and facilitate delivery of equipment.  This meeting may be held in conjunction with the post award conference or identified technical kickoff meeting. The Contractor shall also present the Shipment/Delivery Weekly Progress Report format for review and approval by the Government.  This meeting, if held independently, shall be conducted telephonically within ten days after award and shall incorporate any delivery schedule changes to the draft Delivery Schedule identified by the Government.

Shipment/Delivery Progress Report

The Contractor shall provide a Shipment/Delivery Progress Report which shall identify the items shipped, the serial number associated with each piece of equipment; the date of each shipment; the status of each shipment, tracking information, and information relative to Government-receipt of the equipment items at each delivery site.  In addition, the Shipment/Delivery Weekly Progress Report shall identify any problems and provide a description of how the problems were resolved/addressed.  If problems have not been completely resolved, the Contractor shall provide an explanation and status of resolution.  Shipment/Delivery Progress Reports shall be submitted in Microsoft Excel Format and shall clearly identify each serial number of the equipment being delivered with one (1) serial number per cell.

The Shipment/Delivery Progress Report will be delivered as status changes but no more than frequently than once per week.

Inspection: Destination  
Acceptance: Destination  
Free on Board (FOB): Destination

Packing Slips/Labels and Lists shall also include the following:

IFCAP PO #: \_\_\_\_\_\_\_\_\_\_\_\_ (e.g., 166-E11234 (the IFCAP PO number is located in block #20 of the SF 1449))

Project Description: Enterprise Encryption Key Management System

Total number of Containers: Package \_\_\_ of \_\_\_. (e.g., Package 1 of 3)

Deliverables:

1. Master Delivery Schedule
2. Shipment/Delivery Progress Report

# ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

1. 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](https://www.tms.va.gov/). If you do not have a TMS profile, go to [https://www.tms.va.gov](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.

1. VA Enterprise Architecture Compliance

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

* 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>

1. 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.

* 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

* 1. 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.

* 1. 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.

* 1. 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>.

**Deliverables:**

* + - 1. Final Section 508 Compliance Test Results

1. 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.
6. 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 toProtected 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:
8. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
9. Controlled access to system and security software and documentation.
10. Recording, monitoring, and control of passwords and privileges.
11. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
12. 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.
13. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
14. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
15. Contractor does not require access to classified data.
16. 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.
17. 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.
18. 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](http://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](http://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***

1. 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.

1. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS
   1. 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.
   2. 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.
   3. 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.
   4. 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.
   5. 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.
2. VA INFORMATION CUSTODIAL LANGUAGE
3. 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).
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

Not Applicable

1. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE
   1. 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.
   2. 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.
   3. 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.
   4. 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.
   5. 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.
   6. 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.
   7. 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.
2. SECURITY INCIDENT INVESTIGATION
   1. 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.
   2. 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.
   3. 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.
   4. 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.
3. LIQUIDATED DAMAGES FOR DATA BREACH
   1. 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.
   2. 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.
   3. 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:
      3. date of occurrence;
      4. data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
      5. Number of individuals affected or potentially affected;
      6. Names of individuals or groups affected or potentially affected;
      7. 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;
      8. Amount of time the data has been out of VA control;
      9. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
      10. Known misuses of data containing sensitive personal information, if any;
      11. Assessment of the potential harm to the affected individuals;
      12. Data breach analysis as outlined in 6500.2 Handbook, *Management of Breaches Involving Sensitive Personal Information*, as appropriate; and
      13. 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.
   4. 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.
4. 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-day’s 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.

1. TRAINING
2. 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 cyber security 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.]*
3. 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.
4. 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.