DRAFT

PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS

Office of Information & Technology
Information Technology Operations and Planning

Maintenance and Support of VistA III

Date: March 22, 2018
TAC-19-50570
Task Order PWS Version Number: 3.0

Contents

1.0 BACKGROUND

The mission of the Department of Veterans Affairs (VA), Office of Information Technology (OIT) is to provide benefits and services to Veterans of the United States. In meeting these goals, OIT 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 OIT is responsible for providing maintenance and support services for the Veterans Health Information Systems and Technology Architecture (VistA) and VistA Imaging Operational Environments in VA facilities across the nation, which provide care to Veterans twenty-four hours per day, 365 days per year. The VistA and VistA Imaging environment primarily consists of Hewlett Packard's (HP) proprietary Alpha/Itanium servers running HP's Open Virtual Memory System (OpenVMS) operating system, HP storage systems and NetApp storage systems. These mission critical systems provide storage and access for electronic medical records for all patients treated at VA facilities. Operational anomalies and downtime of these systems are considered life-threatening situations as timely access to mission critical electronic medical records directly impacts patient care. Access to In-Depth engineering support for both Alpha/Itanium hardware and OpenVMS, such as Operating System internals modifications and direct Alpha firmware modification, are critical for operational stability and for quick restoration of failed systems.

2.0 APPLICABLE DOCUMENTS

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

1. 44 U.S.C. § 3541-3549, "Federal Information Security Management Act (FISMA) of 2002"
2. "Federal Information Security Modernization Act of 2014"
3. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
4. FIPS Pub 199. Standards for Security Categorization of Federal Information and Information Systems, February 2004
5. FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems, March 2016

6. FIPS Pub 201-2, “Personal Identity Verification of Federal Employees and Contractors,” August 2013
7. 10 U.S.C. § 2224, "Defense Information Assurance Program"
8. 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
9. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
10. Public Law 109-461, Veterans Benefits, Health Care, and Information Technology Act of 2006, Title IX, Information Security Matters
11. 42 U.S.C. § 2000d “Title VI of the Civil Rights Act of 1964”
12. VA Directive 0710, “Personnel Security and Suitability Program,” June 4, 2010, http://www.va.gov/vapubs/
13. VA Handbook 0710, Personnel Security and Suitability Security Program, May 2, 2016, http://www.va.gov/vapubs
14. VA Directive and Handbook 6102, “Internet/Intranet Services,” July 15, 2008
15. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
16. Office of Management and Budget (OMB) Circular A-130, “Managing Federal Information as a Strategic Resource,” July 28, 2016
17. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
18. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
19. 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
20. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
21. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, 2012
22. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” March 10, 2015
23. VA Handbook 6500.1, “Electronic Media Sanitization,” November 03, 2008
24. VA Handbook 6500.2, “Management of Breaches Involving Sensitive Personal Information (SPI)”, July 28, 2016
25. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring Of VA Information Systems,” February 3, 2014
26. VA Handbook 6500.5, “Incorporating Security and Privacy in System Development Lifecycle”, March 22, 2010
27. VA Handbook 6500.6, “Contract Security,” March 12, 2010
28. VA Handbook 6500.8, “Information System Contingency Planning”, April 6, 2011
29. OI&T Process Asset Library (PAL), https://www.va.gov/process/ . Reference Process Maps at https://www.va.gov/process/maps.asp and Artifact templates at https://www.va.gov/process/artifacts.asp

30. One-VA Technical Reference Model (TRM) (reference at https://www.va.gov/trm/TRMHomePage.aspx)
31. VA Directive 6508, "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 15, 2014
32. VA Handbook 6508.1, "Procedures for Privacy Threshold Analysis and Privacy Impact Assessment," July 30, 2015
33. VA Handbook 6510, "VA Identity and Access Management", January 15, 2016
34. VA Directive 6300, Records and Information Management, February 26, 2009
35. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
36. NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach, June 10, 2014
37. NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, January 22, 2015
38. OMB Memorandum, "Transition to IPv6", September 28, 2010
39. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015
40. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 24, 2014
41. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
42. OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies, December 16, 2003
43. 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
44. 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
45. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
46. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
47. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
48. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
49. NIST SP 800-63-3, 800-63A, 800-63B, 800-63C, Digital Identity Guidelines, June 2017
50. NIST SP 800-157, Guidelines for Derived PIV Credentials, December 2014
51. NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012

52. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
53. 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)
54. 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)
55. VA Memorandum "Mandate to meet PIV Requirements for New and Existing Systems" (VAIQ# 7712300), June 30, 2015, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4846
56. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, Department of Homeland Security, October 1, 2013, https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf
57. OMB Memorandum M-08-05, "Implementation of Trusted Internet Connections (TIC), November 20, 2007
58. OMB Memorandum M-08-23, Securing the Federal Government's Domain Name System Infrastructure, August 22, 2008
59. 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)
60. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
61. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
62. Executive Order 13693, "Planning for Federal Sustainability in the Next Decade", dated March 19, 2015
63. Executive Order 13221, "Energy-Efficient Standby Power Devices," August 2, 2001
64. VA Directive 0058, "VA Green Purchasing Program", July 19, 2013
65. VA Handbook 0058, "VA Green Purchasing Program", July 19, 2013
66. Office of Information Security (OIS) VAIQ #7424808 Memorandum, "Remote Access", January 15, 2014, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
67. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
68. 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
69. 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

70. 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
71. "Veteran Focused Integration Process (VIP) Guide 2.0", May 2017, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371
72. "VIP Release Process Guide", Version 1.4, May 2016, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4411
73. "POLARIS User Guide", Version 1.2, February 2016, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4412
74. VA Memorandum "Use of Personal Email (VAIQ #7581492)", April 24, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
75. VA Memorandum "Updated VA Information Security Rules of Behavior (VAIQ #7823189)", September, 15, 2017, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28

3.0 SCOPE OF WORK

The Contractor shall provide the full range of technical, managerial and administrative services to the VA in support of its VistA and VistA Imaging Systems engineering, maintenance, sustainment and logistic requirements. The required services include engineering support and engineering changes, updates, repairs, and other technical services involving the VistA and VistA Imaging Systems Alpha/Itanium processors, OpenVMS operating systems, and ancillary hardware and software as well as providing all support required for maintenance and continuity of operation services, without voiding warrantees and/or the operational integrity of the Vista and Vista Imaging systems across the VA enterprise. There are approximately 143 VistA facilities including numerous VA Medical Centers, VA Veterans Integrated Service Network (VISN) data centers, and Regional Data Processing Centers operating hundreds of Alpha/VMS-based systems in support of VistA Platforms throughout the United States, as well as San Juan, PR and Manila. The Contractor shall also provide sufficient program management services to manage and deliver service levels that minimize solution deliver times, costs and problems and consistently deliver quality products to meet business requirements.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance shall be 12 months from date of award, with four (4) 12-month option periods.

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

Under current definitions, four are set by date:

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

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

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

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

4.2 PLACE OF PERFORMANCE

Efforts under this contract shall be performed at Contractor facilities and VA facilities. The Contractor shall identify the Contractor's place of performance in their Task Execution Plan submission.

4.3 TRAVEL

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

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.1 PROJECT MANAGEMENT-

5.1.1 MONTHLY PROGRESS REPORT

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

The Monthly Progress Reports shall cover all work completed during the reporting period and work planned for the subsequent reporting period. The report shall also identify any problems that arose and a description of how the problems were

resolved. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving the issue. It is expected that the Contractor will keep in communication with VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

In addition to the information required above, throughout the PWS there are task outputs that are required to be "included in the Monthly Progress Report" Details of each of these can be found in their respective requirement section. Below is a summary reference list of the applicable sections and information required:

a) 5.2.1 Site-Visit Reports
b) 5.2.2 Routine Hardware Maintenance Activity summary
c) 5.2.4 Component Inventory Changes Report
d) 5.3.1 Call Report Daily Summary
e) 5.3.2 Aggregated and tabulated Call Report Daily Summary
f) 5.4.1 Monthly Software Change Documentation Report
g) 5.4.2 Monthly Software Sustainment Change Documentation Report
h) 5.4.3 Monthly Patch Activity
i) 5.6.3.2 O&M Status Update for Recoverall Maintenance
j) 5.6.3.3 Recover Inventory Changes report

Deliverable:

A. Monthly Progress Report

5.2 COMPONENT MAINTENANCE SUPPORT SERVICES

Due to the mission critical nature of the VistA and VistA Imaging systems, VA's objective is to ensure these systems are operational and accessible without interruption. The Contractor shall ensure that the VA's inventory of VistA and VistA Imaging systems and all their components as listed in PWS-Attachment-B-General Inventory are maintained in a state of readiness and operation. To that end, Severity Levels have been set by the Government.

5.2.1 Severity Levels.

All calls during business hours, 0700 Eastern Time through 2100 Eastern Time Monday through Friday excluding Government Holidays, shall be answered immediately via the Contractor-established VA-Dedicated support center (5.3). Calls after-hours shall be answered within 30 minutes. All Maintenance and support operations shall be 24x365 based as VA operates critical patient care on a 24x365 bases.

At the onset of the initial call, the severity level shall be determined via the following guidelines in the severity level table. While the contractor may suggest a severity level,

the Government employee calling for support shall have the final say in Severity level determination.

Government reserves the right to escalate a severity level determination should circumstances warrant it. For example, a damaged drive (routine, Level 4) has begun to affect the storage sub-system (level 1 or 2)

Severity Level	Description	Problem Determination	Problem Resolution Expected
1	Operations have either been compromised or have ceased. Patient care is, or is immediately subject to compromise.	1 hour	2 hours
2	Operations have been compromised but continue to function adequately. Patient care is subject to compromise but is not imminent.	1 hour	4 hours
3	Operations continue and are only slightly impaired. Patient care is not in danger or compromised.	4 hours	1 business day
4	Problem is routine. Problem is not significantly impacting operations and continue unaffected. Patient care is not in any danger whatsoever.	8 hours	5 business days

The contractor shall provide continuous updates to the parties involved. In the event the contractor fails to meet these timeframes, the contractor shall:

1) Create a Service Shortage Memo to explain why and what actions will be taken to correct in future.
2) Contact involved parties, providing explanation.
3) Escalate the problem internally to bring additional resources to bear on the problem.
4) Document what actions will be taken to ensure the service shortage will not be repeated.

The component maintenance support services are predicated on the maintenance of the component inventory provided in PWS-Attachment-B-General Inventory.

5.2.2 Break-Fix Services

The Contractor shall provide break-fix support services and remote troubleshooting as well as providing for on-site repair support and parts for VistA and VistA Imaging Systems via a request for support from the Expertise Center (see section 5.3) or Break-Fix Service requests directly from the VA PM or COR.

During break-fix efforts, the Contractor shall:

1. Identify any needed parts prior to a site visit and ensure their availability when responding to an on-site Break-fix call.

2. Ensure the proper operation of Recoverall and other Vista and Vista Imaging Systems throughout the VA enterprise.

3. Conduct all hardware repairs and problem resolutions with continuous effort. Continuous effort means that once notified that a problem exists, The Contractor shall work uninterrupted until the problem is resolved.

The Contractor shall respond in accordance to section 5.2.1. Response time on a maintenance request shall begin when the request for break-fix service is placed by the Expertise Center, VA PM, or COR. The Contractor shall track break-fix service requests from receipt until closure and report their status in the Monthly Progress Report.

If the Contractor conducts any site visit for resolution of problems, a summary site-visit report shall be submitted outlining the aspects of the problems that required the visit and their solutions as well as any required follow-on actions and recommendations to VA COR and VistA and VistA Imaging PM. The Contractor shall also incorporate these site-visit reports as attachments to the Monthly Progress Report.

5.2.3 Hardware Maintenance

The Contractor shall provide routine hardware maintenance for the entire VistA configuration at all applicable VistA and VistA Imaging installations as identified in Attachment-B-Locations. All activities conducted for routine hardware maintenance shall be summarized in a “Routine Hardware Maintenance Activity Summary” in the Monthly Progress Report.

5.2.4 Parts Supply

The Contractor shall provide all repair parts and supplies necessary to perform Break-Fix activities and ensure the continuous operation of the VA’s VistA and VistA Imaging Systems throughout the duration of this effort. The Contractor shall:

1. Provide parts that comply with VistA and VistA Imaging Systems Original Equipment Manufacturer (OEM) guidelines and that do not void manufacturer’s warrantees.
2. Have part supplies in quantities sufficient to service all VistA and VistA Imaging Systems locations in compliance with the parameters of this contract.
3. Ensure their continuity of operations plans include contingencies that shall ensure meeting the terms of this contract under emergency conditions such as natural disasters.

4. Ensure parts for the VA's VistA and VistA Imaging Systems are available throughout the life of effort, including items anticipated to be deemed end of service life during the performance of this contract.

With the concurrence from the COR or VA PM if equipment is deemed to be at the end of its useful life or beyond repair, serviceable used parts from the VistA and VistA Imaging Systems shall be removed from the VistA Systems. These parts shall be recycled by the Contractor as Government Furnished Equipment (GFE). These available parts shall be delivered to VA for use at VA's discretion.

5.2.5 Component Inventory Support

The Contractor shall inventory all component equipment being maintained. The initial component inventory is provided in PWS-Attachment-B-General Inventory The Contractor shall perform quarterly physical inventories of GFP and provide the changes from the previous quarter to the VA as the "Component Inventory Changes Report", included as an attachment to the Monthly Progress Report. The Contractor shall prepare a Component Inventory Auditing Methodology Plan. This plan shall be used to audit Government Component Inventory Property (PWS-Attachment-B-General Inventory) and provide a metric to determine the percentage gain/reduction in the component inventory from the previous yearly inventory. The accuracy of the inventory shall exceed 95%. At VA's discretion, the CO/COR may reduce the frequency of physical inventories to not less than every 180 days. The contractor shall compile a complete Component inventory report semi-annually.

Within 30 days of contract award, the contractor shall provide a Contract-Exclusive User/Password protected Internet Portal (Web Browser Accessible) system for VA viewing of the current VA MSV inventory. This Web Portal shall provide a means for VA employees to request access and access shall only be granted to individuals with @va.gov TLD domain email addresses. The contractor shall maintain the currency status of this web portal to within 14 days of any updates performed or received. Accounts for the contract COR, Assistant COR, PM and CO shall be generated with access information emailed to each. The Contractor shall provide written instructions for access and use of this portal to the contract COR in electronic form and users that need access.

Deliverables:

A. Component Inventory Auditing Methodology Plan
B. Complete Component Inventory report
C. Inventory Portal initial access account information
D. Instructions on access and use of the Inventory Portal

5.3 EXPERTISE CENTER TECHNICAL SUPPORT

The Contractor shall establish and fully support an Expertise Center which serves as the single point of contact for reporting, managing, monitoring, and correcting problems with the operation of the Vista and VistA imaging Systems throughout the VA Enterprise. This support shall encompass a broad range of software and hardware products that integrate with VistA and VistA Imaging including but not limited to; OpenVMS, Windows, Linux and Intersystems Cache.

This Expertise Center support shall include:

- Call Center Help Desk Support
- Infrastructure Management Support
- Technical Performance Management Support
- Operations and Problem Resolution Support

5.3.1 Call Center Help Desk Support

The Contractor shall perform activities required to provide incident detection and recording, classification and initial support, investigation and diagnosis, resolution and recovery, incident closure or incident escalation (problem ticket), incident ownership, monitoring, tracking and communication. Incidents are captured at the time the user contacts the help desk. The outputs of this process are resolved and closed incidents, change requests, or problem tickets.

The Contractor shall support Vista and VistA Imaging Systems Help Desk activities that include:

a. Responding to reported incidents
b. Responding to general service requests
c. Diagnosing and implementing recovery steps
d. Providing communications to requestors and other parties
e. Completing incident closure
f. Completing problem escalation and incident tracking.

To perform this task, the Contractor shall provide a dedicated toll free telephone number and a dedicated email inbox both operating 24 hours per day. The toll-free number shall be staffed from 0700 Eastern Time through 2100 Eastern Time Monday through Friday excluding Government Holidays. After hours, weekends and Government Holidays, the Contractor shall provide a call back response to the customer within 30 minutes of receipt of a call for high priority and/or emergency needs (A High Priority/Emergency situation is defined as a situation that involves current or imminent downtime for VistA or VistA Imaging Operations as outlined in 5.2.1.) The Contractor shall maintain a record of all incoming calls and emails for input into the Call Report Daily Summary. There are an estimated 25 calls per day. The summary shall also

include resolution information. The information to be logged into the summary for each contact shall include:

i. Date/time call originated
ii. Origination individual
iii. Originating facility
iv. Priority
v. Nature of call
vi. Initial technician
vii. Progress notes
viii. Final resolution
ix. Resolution date/time
x. Approximate man hours spent resolving the problem.

All Call Report Daily Summary information for each month shall be aggregated and tabulated and included as an appendix to the Monthly Progress Report.

5.3.2 Infrastructure Management and Support

The Contractor shall ensure availability and reliability of the VistA and VistA Imaging Systems across the VA Enterprise. The Contractor shall be responsible for maintaining infrastructure support from the physical server to the Operating System and application software and shall be responsible for the overall continuity management for VistA and VistA imaging, as well as for the backup and recovery of the infrastructure (restoring server operations up to the operating system and application level).

The Contractor shall coordinate routine and recurring infrastructure support activities required to ensure VistA and VistA imaging maintains production and non-production instances at the VA Facilities listed in the related attachment.. The environments shall be maintained to meet the availability, reliability, continuity, and security requirements (as defined by consistently updated VA Security policies), needed by the VistA and VistA Imaging Systems and the VA Enterprise. In addition, the Contractor shall provide technology review and assessment support in order to review technical emerging infrastructure changes, technology changes related to VA enterprise architecture or other improvements impacting VA VistA and VistA Imaging Systems, and attend meetings as necessary, anticipated to be 1 or 2 per year, to review planned and emerging requirements and provide configuration recommendations.

Infrastructure Management Support activities for VistA and VistA Imaging Systems shall include:

1. Providing support to configure, maintain, monitor performance, test, diagnose, and resolve problems for all VistA and VistA imaging hardware and software components remotely or on-site as required.

2. Providing technical support for the design, operation, upgrading, and reconfiguration of all VistA and VistA Imaging systems.

3. Supporting life-cycle baseline technical and functional planning and development

4. Providing support to develop new, and maintaining, modifying and integrating as required, existing application (enterprise and local) systems in accordance with and approval of the VA VistA and VistA Imaging PM and the COR.

5. Maintaining the inventory of VA VistA Systems Resources based on PWS-Attachment-B-General Inventory.

Infrastructure management activities shall be aggregated and summarized in the Monthly Progress Report.

5.3.3 Operations and Problem Resolution Support

5.3.3.1 Hardware and Software Troubleshooting Support

The Contractor shall provide hardware and software troubleshooting support for the VistA Systems. These systems include Alpha-Based CPU's, VMS operating Systems, Linux Operating Systems, and limited x86-Based CPU's as well as all other hardware and software components of the VistA/VistA Imaging Systems The Contractor shall perform remote operations via secure communication methods. Performance and/or configuration problems, that persist for an extended period shall be resolved using supplemental on-site support provided through the Expertise Center

5.3.3.2 Break/Fix Coordination Support

The Contractor shall perform Break/Fix tasks support of VistA and VistA Imaging systems as tasked by the Expertise Center. This includes coordinating on-site support of field service technicians including dispatch, monitoring, and repair for components found in PWS-Attachment-B-General Inventory and taking all necessary action to restore a troubled system to full operational capacity as soon as possible. As with Non-Expertise center generated Break/Fix tasks, the Contractor shall work on a continuous effort basis until the problem is corrected giving the highest priority to resolution of the problem and working on the issue uninterrupted until it is resolved.

5.3.4 Escalation Plan Support

The Contractor shall create an escalation plan that identifies all procedures from problem initiation through coordination of all actions necessary to correct a problem and to return the VistA/VistA Imaging Systems to a fully operational state as soon as possible. This may mean escalating the problem within the Contractor's organization, within the VA other engineering groups as required (hardware, software, and suppliers).

In the event operational outages are not being addressed in a satisfactory manner as determined by the COR or CO, this escalation plan will be put into effect.

Deliverable:

A. Escalation Plan

5.3.5 VistA Imaging Qualification Lab and Support

The VistA Imaging Solution is an FDA approved medical device requiring rigorous testing and qualification in order to maintain its FDA approved medical device status. The Contractor shall provide a VA-dedicated VistA Imaging Qualification Lab (IQL) for testing and qualifying Imaging solutions for FDA approval. The Contractor shall conduct extensive and rigorous testing of any vendor submitted hardware and software configurations based on test procedures provided by VA Imaging Development Team. The Contractor shall perform testing by rigorously following FDA testing and qualification procedures. The Contractor shall provide a report compiling and analyzing the results of each solution testing effort. This task is anticipated to be utilized by various VistA Imaging efforts being worked on by the VistA Imaging Team.

Deliverable:

A. IQL testing results reports for submitted candidate VistA Imaging Solutions

5.4 SOFTWARE MANAGEMENT SUPPORT

5.4.1 Infrastructure Software Upgrade Support

The Contractor shall perform activities related to the supporting of VistA Platform infrastructure software such as firmware, drivers, interfaces, operating systems, etc. as listed in Attachment-B-General Inventory to build/remediate interfaces, extensions, or enhancements to satisfy the VA business requirements or to fix current software that have defects. The Contractor shall ensure that changes are recorded, prioritized, planned, authorized, developed, unit and integration tested, and documented in accordance with established configuration management plans. Software Maintenance includes modification of a software system or component after delivery to correct faults, improve performance or other attributes; adapt to a changed environment or maintenance activities focused on anticipated problems, or preventive maintenance.

5.4.2 Infrastructure Software Sustainment Support

The Contractor shall provide Software sustainment support. This sustainment support includes processes, procedures, expertise, material, and information required to support, maintain, and operate the infrastructure software aspects of the VistA and VistA Imaging systems. It includes sustaining engineering, configuration management, training, survivability, environment, and protection of critical program information, anti-tamper provisions, IT security, supportability and interoperability functions, COTS product management, and technology refresh. The Contractor shall ensure that

changes are recorded, prioritized, planned, authorized, developed, unit and integration tested, and documented in accordance with established VistA and VistA Imaging Configuration Management procedures.

5.4.3 Infrastructure Application Patch Management Support

The Contractor shall be responsible for ensuring all VistA and VistA Imaging environments are kept in an active and mirrored state. VistA and VistA Imaging environments include production servers, pre-production servers, test servers, recoverall and training servers. This responsibility shall include performing activities required to plan, evaluate, design, test, schedule, and deploy service patches/hot fixes to address application, tools, bolt-ons and related components within the VistA and VistA Imaging System.

Activities include, but are not limited to:

1. Technical Impact Analysis
2. Deployment after approval by VA PM
3. Validation and unit testing to include regression and system integration testing
4. Documentation of status in the Monthly Progress Report of all patches deployed or under consideration for deployment
5. Configuration Management

Patch activities described above shall be documented in a Monthly Patch Activity Report and included in the Monthly Report.

5.5 RECOVERALL SUPPORT

The mission critical nature of the current VistA and VistA Imaging operational environment requires VA to have backup systems available in the event of an emergency or catastrophic event. The Contractor shall maintain a fully updated, operational and tested system available at all times, ready to ship immediately upon request by VA. This system is referred to as “Recoverall.” This Recoverall system shall have the ability to operate VistA or VistA Imaging operations at any VA Medical Center or facility excluding the Regional Data Processing Center (RDPC) installations. Over the life of the MSV contract from 2008 to 2018, Recoverall has been invoked 4 times. As the equipment in the field ages, we expect this to grow at least one event per year.

The Contractor shall obtain critical data, processes, service level requirements, and plans to enable VistA and Vista Imaging resources (Recoverall) at a target recovery location. The Contractor shall recommend best practice VistA and Vista Imaging Service Continuity and Recoverall strategies, policies, and procedures and develop and maintain a detailed VistA and Vista Imaging Service Continuity and Recoverall plan to achieve customer VistA and Vista Imaging Services Continuity and Recoverall requirements. This plan shall include data, back-ups, hardware/software, storage

management, deployment, and contingency operations that provide for recovering customer's VistA/VistA Imaging systems within required recovery timeframes after a disaster affects customer's use of the Services, as well as plans for restoration of customer VistA and Vista Imaging Systems and Services that are critical for supporting Customer business operations. The Contractor shall execute the VistA and Vista Imaging Service Continuity and Recoverall plan and notify and guide the customer per Recoverall plans, policies and procedures. Events that would necessitate the execution of this plan include any events that severally impede or terminate the operation of the VistA/VistA Imaging platform.

Deliverable:

A. Updated VistA and Vista Imaging Service Continuity and Recoverall plan

5.5.1 Baseline

The Contractor shall complete a top-down architecture assessment and Systems Engineering (SE) analysis of the complete VistA and VistA Imaging System using the VA-provided inventory in PWS-Attachment-C-Recoverall as a starting point. This assessment shall include:

1. System engineering reviews and analyses of current architecture, design, and implementation to document and baseline current VistA and VistA Imaging systems. This effort shall be documented in a Baseline VistA and VistA Imaging System Documentation Report.
2. System engineering assessments and recommendations to simplify or remove unnecessary or unused applications and/or hardware and software without impacting VistA and VistA Imaging System performance
3. System engineering assessments and recommendations for implementing additional emerging technologies or techniques to improve or augment functionality, stability, reliability, scalability, and flexibility of the VistA and VistA Imaging System

The results of the second and third reviews and analyses listed above shall be documented in a Detailed Engineering Analysis Results Report.

Deliverable:

A. Baseline VistA and VistA Imaging System Documentation Report
B. Detailed Engineering Analysis Report

5.5.2 Augmentation

The Contractor shall monitor configuration changes and updates to the VistA and VistA Imaging Baseline System in order to prepare an annual Recommendation For Augmentation Report. For each element with a proposed update/change, the Contractor shall provide the following information in the Recommendation For Augmentation report including:

1. A problem statement
2. description of the proposed upgrade/change
3. A list of alternatives considered
4. An Analysis showing how the upgrade/change will solve the problem and not introduce new problems
5. Verification of interface compatibility (including impacts on test, operations, safety, reliability, etc.)
6. Estimate impacts to Recoverall (costs, schedules, etc.)
7. Preparation of a Bill of Materials (BOM) for VA's review of costs to implement the various elements of the proposed upgrade/change
8. Identification of the impact if upgrade/change is not implemented.

Should VA execute any or all of the recommendations, Government furnished equipment (GFE) may be provided to the Contractor for installation and integration into the Recoverall System. The Contractor shall then implement the approved upgrades and/or changes or arrange for the upgrade and/or change in a manner that maintains the integrity of all relevant warrantees to bring the Recoverall system configuration to a condition in which they are capable of meeting all operational and functional requirements for which they were designed. To accomplish this, the Contractor shall furnish all required labor, facilities materials, fixtures, equipment, tools, test equipment, technical data/expertise and all other facilities necessary to provide Recoverall upgrade/change services. Once approved changes/upgrades are complete, the upgraded systems shall be returned to the Recoverall inventory of available systems

Once installed, and fully integrated, the Contractor shall update all configuration documents and procedures and maintain this augmented equipment as an integral part of the Recoverall system in the appropriate manner (i.e. manufacturer's warranty, break/fix, etc.).

Deliverable:

A. Bill of Materials that meets the need for the recommendations.

5.5.3 Recoverall Storage, Maintenance, and Inventory

5.5.3.1 Recoverall Storage

The Contractor shall provide facilities appropriate for the storage and operation of the Recoverall Systems. The Contractor shall ensure these facilities provide all necessary services to support all Recoverall activities such as power, networking, space, heating and cooling. The Contractor shall provide secure storage of all Government Furnished Property (including Recoverall Systems, Ancillary Hardware and Software, Cables, Connectors, Parts Reserve, etc.) in accordance with VA Department of Property Management policy and applicable regulations.

5.5.3.2 Recoverall Maintenance

The Contractor shall be responsible for end-to-end Recoverall systems operations and maintenance (O&M) services including hardware and software installation, systems administration, systems upgrades, preventive and corrective maintenance, and incident management. The maintenance shall be performed on the Recoverall systems until system retirement.

The Contractor shall provide a Monthly O&M Status update to be included in the Monthly Progress Report that lists and describes patches, upgrades, updates and all applicable maintenance activities for the Recoverall Systems.

The Contractor shall perform the following type of activities as appropriate:

1. Administer, manage, and maintain the Recoverall System VistA and VistA Imaging and production environments to ensure they are as closely configured to the production installation as possible.
2. Support implementation and testing of all development enhancements and releases as well as all application upgrades, updates, and manufacturer released security patches
3. Plan and execute any needed upgrades to the software applications and maintain licensing integrity
4. Support installation of operating systems, database, COTS products, applications development upgrades and new releases
5. Schedule and execute regular system administrative activities, including system reboot, back up, recovery, archiving and restoration
6. Protect the Recoverall System from unauthorized software, middleware, or hardware upgrades

5.5.3.3 Recoverall Inventory Support

The Contractor shall inventory equipment and software and maintain an accurate inventory of Recoverall systems and parts that are available for use. The Contractor shall perform monthly physical inventories of GFP and provide the changes from the previous month to the VA as the “Recover Inventory Changes Report”, included as an attachment to the Monthly Progress Report. The Contractor shall prepare Inventory Auditing Methodology Plans. This plan shall be used to audit Government Property the accuracy of the inventory shall exceed 95%. At VA’s discretion, the CO/COR may reduce the frequency of physical inventories to not less than every 90 days. The contractor shall compile a complete Recoverall System inventory report semi-annually.

Deliverables:

A. Auditing Methodology Plan
B. Complete Recoverall Inventory report

5.5.4 Recoverall System Laboratory Support

The Contractor shall create, support, and maintain a VistA and VistA Imaging testing laboratory for the primary purpose of replicating, analyzing, and troubleshooting, VistA

and VistA Imaging System Environment problems. This testing shall make maximal use of the inventory of Recoverall Systems available in inventory. Additionally, the VistA and VistA Imaging testing laboratory shall:

1. Operate as a test environment for designing, configuring, testing, and integrating new technologies, software, and components in the VistA environment.
2. Support the performance of Engineering Investigations to solve unique VistA and VistA Imaging System Environment problems
3. Be used to train VistA and VistA Imaging System support personnel in the operations of the VistA and VistA Imaging System. Training shall encompass, at a minimum, theory of operations, system setup/initialization, operations, and troubleshooting.
4. Be used to review and assess modifications and potential modifications of the overall VistA and VistA Imaging System design to maximize effectiveness in Recoverall situations while maintaining its overall operational integrity.

The Contractor shall make this lab available to VA personnel between 8 AM and 5 PM Eastern, Monday through Friday (excluding Government holidays) to both inspect and utilize these systems for both testing and experimentation.

5.5.5 Recoverall Invocation Support

At the onset of an emergency or catastrophic event, authorized VA Personnel (COR or Authorized Technical Representatives as designated by the COR) will invoke Recoverall operations. When Recoverall is invoked, the Contractor shall make and provide a telephonic/email functional assessment of the target site's problems, which shall include an assessment of existing infrastructure and practices, analysis of the target site's current configuration and current and projected business volumes, and system performance requirements. The Contractor shall complete an analysis and an up-to-date assessment of Recoverall system availability and suitability to meet the target site's needs.

Under extraordinary circumstances, such as the Contractor discovers a catastrophic situation, or field facility personnel are not available, the Contractor may also contact an Authorized Government representative to request Invocation authorization. Points of contact will be provided at time of contract award.

In either case, the Contractor shall brief the appropriate VA Personnel as to the nature and reason for the Invocation request and provide a current situation analysis. The analysis shall include at a minimum the following components:

1. Fitness of the available Recoverall hardware and software system to support the expected business function, anticipated volumes, maintainability and performance criteria, and reliability requirements of the target site
2. Any recommended changes to the existing Recoverall hardware and software configuration necessary to achieve better congruence with aforementioned target site's requirements
3. Implementation of approved changes (prior to or post shipment)

The Contractor shall include the above analysis in the Recoverall Situation Post Deployment Report and also include relevant documentation, timestamps for all calls, emails and other remediation response timelines.

Deliverable:

A. Recoverall Situation Post Deployment Report

5.5.5.1 Recoverall System Selection and Equipping Support

The Contractor shall obtain a Recoverall System from the available inventory, update any required software, equip the Recoverall System with a set of the required cables, connectors, mounts, consumables and any necessary hardware and software and prepare it to be shipped to the target site where the broken equipment is located.

5.5.5.2 . Recoverall System Packing and Packaging Support

The Contractor shall properly pack the Recoverall equipment selected for shipment to the target facility. The Contractor shall package the Recoverall System and all required cables, connectors, mounts and ancillary hardware/software/consumables necessary for operation in a way suitable for protecting them during shipping as well as allowing for re-use to the maximum extent possible for the return of the Recoverall System to the Contractor. Packing, packaging, and marking shall be accomplished by the Contractor in accordance with standard commercial practices. The items shall be inspected and must be in good working condition prior to acceptance at destination.

5.5.5.3 . Recoverall System Shipping Support

The Contractor shall arrange for shipment of the Recoverall System to the designated location via the most expeditious means that maintains the integrity of the equipment being shipped (i.e., truck, air freight, private courier). The Contractor shall ensure Authorized Government representatives are appropriately notified of each shipment and shall also ensure that all Recoverall Systems are properly tagged as such. The equipment shall be shipped within 8 hours of Recoverall Invocation and must be on-site at the designated location within 24-48 hours. Exceptions to this timeline must be approved by the COR or other Authorized Government representative. The Contractor shall also provide shipment tracking information (tracking numbers, etc.) to the COR and to each Authorized Government representative via email as proof of delivery.

The Recoverall Packing Slip must be included in each package of a shipment and, as a minimum, shall include the following information (as appropriate):

1) Item Name(s)
2) Item Description
3) Make
4) Model
5) VA Property Asset Tag Number
6) Serial Number(s)
7) Quantity
8) Ship To Address
   a) Name
   b) Routing Information / Street Address
   c) City, State
   d) Zip Code
   e) Phone Number
   f) Point of Contact Name
9) Ship From Address
   a) Name
   b) Routing Information / Street Address
   c) City, State
   d) Zip Code
   e) Phone Number
   f) Point of Contact Name
10) Tracking Number
11) Date Shipped
12) Shipping Point of Contact Name and Phone Number

As necessary, to facilitate the Recoverall Process, the Contractor shall provide ancillary Recoverall Shipping Support to include receiving, inventorying, preparation, packaging, shipping, integration and disposition services in accordance with all applicable best practices, directives, guidance and laws.

Deliverables:
A. Shipping Tracking Information
B. Fully Updated Packing Slips

5.5.5.4 Recoverall Installation/Recovery Operations Support

Once the shipments have arrived at the target site, the Contractor shall install the Recoverall System and restore the VistA and VistA Imaging systems to full operation.

As a part of this activity, the Contractor shall:
1) Work cooperatively and in conjunction with VA Support teams
2) Identify utilities, networks, and any other infrastructure support required for installation and operation. The Contractor shall use all existing cable pathways and

hardware including cable trays, raceways, j hooks, conduit, other suspension media, penetrations, and openings to the fullest extent possible.
3) Document all connections between the Recoverall System and the facility infrastructure.
4) Install all system wiring necessary to interconnect system components. All connections to the hospital data network shall be identified and quantified.
5) Provide all necessary engineering and technical support for the Recoverall installation effort
6) Identify and provide needed materials, equipment, and supplies for Recoverall site installations
7) Perform the installation of the Recoverall System at the target site and verify proper operation of the system through testing, analysis, and other applicable means.
On a periodic basis not less than once per 24 hours or as determined between the Contractor and the Authorized Government representative, the Contractor shall report to the CO, COR, and Authorized Government Representatives the status of the deployment and recovery operations.

Deliverable:

5.5.5.5 A. Assessment and Recovery Report Recoverall Post-Event Disposition Support

Once the target site is restored to operational status, the Contractor shall support VA in disposition of all VistA and VistA Imaging equipment replaced by the Recoverall System. This support shall include Repair, Restoration and Replacement support.

5.5.5.5.1 Recoverall Equipment Repair and Restoration Support

The Contractor shall perform an assessment of the VistA and VistA Imaging System replaced by the Recoverall System to determine its operational status and the status of all components and software. If the VistA and VistA Imaging system equipment is assessed to be repairable, the Contractor shall ship the equipment back to the Recoverall Equipment Storage Facility and commence repair of the damaged equipment IAW section 5.2 Break/Fix support

Once repaired, the Contractor shall add the system to the available inventory of available Recoverall systems, replacing the equipment sent during invocation, in order to return Recoverall to full operational capacity as soon as possible. Once accomplished, the Contractor shall update all inventories and applicable documentation to reflect this activity.

5.5.5.5.2 Recoverall Equipment Replacement Support

Should the Contractor's assessment of the VistA and VistA Imaging system equipment replaced by the Recoverall System in the emergency be determined to be irreparable or not cost effective to repair, the Contractor shall prepare a Recoverall Replacement Bill Of Materials (BOM) within one (1) week of full system restoration listing all elements

required for replenishing the Recoverall inventory with a Recoverall System reflecting the most recently accepted baseline.

Deliverable:

A. BOM For Recoverall Restoration

5.5.6 Recoverall and VistA and VistA Imaging System Testing Support

The Contractor, in conjunction with VA Support teams as appropriate, shall verify through testing, that all VistA and VistA Imaging System functions and interfaces are operational and all data is transferred to and from the appropriate system according to the business requirement. The Contractor shall also ensure that it complies with all VA security protocols. The Contractor shall provide VA with a copy of the test methodology, test data, and test results.

During the testing, the Contractor shall verify that the Recoverall System is fully operational and meets all the performance requirements. The Contractor shall test and verify that all system functions and requirements are met and operational.

The Contractor shall conduct the following tests of Recoverall Systems:

1. Test each Recoverall System after installation at target site as part of recovery operation
2. Test each Repaired System after Break/Fix repair
3. Conduct regularly schedule tests of Recoverall Systems in inventory (not less than once every 60 days)

The Contractor shall submit the test results and certification of full operation to the VA PM and COR for acceptance.

Deliverables:

A. Test Methodology, Test Data, and Test Results
B. Certification of full operation

5.6 PHASE IN PLAN

The Contractor is expected to participate in Phase-In discussions/meetings and work closely with MSV staff and the current out-going MSV Contractor(s) to work out any residual transitioning topics to kick start this contract. The Contractor(s) shall transition all services in 120 days.

The Contractor shall provide a detailed transition plan that includes:

5.6.1.1.1 Roster of key POCs with name, role, email address, and telephone numbers.
5.6.1.1.2 Transition timeline with key milestones.

5.6.1.1.3 Procedural manuals/guidelines.
5.6.1.1.4 Templates used in day-to-day operations.
5.6.1.1.5 Itemized list of additional equipment to be provided.
5.6.1.1.6 Process for transfer of on-hand inventory, if applicable.
5.6.1.1.7 Process for transfer of GFE/Recoverall inventory
5.6.1.1.8 Transition checklist.
5.6.1.1.9 Signed turnover agreements, if applicable.
5.6.1.1.10 System design plan.
5.6.1.1.11 Network architecture plan.

DELIVERABLE:

A. Phase-In Transition Plan (Offerors proposed Phase-in Plan will be incorporated into the task order upon award.)

5.7 PHASE OUT PLAN

At the end of this contract, the Contractor is expected to participate in Phase-Out discussions/meetings and work closely with MSV staff and the incoming Contractor(s) to work out any residual transitioning topics require to help kick start the future contract.

The Contractor shall provide a detailed Phase-Out Transition Plan that includes:

5.7.1.1.1 Roster of key POCs with name, role, email address and telephone numbers.
5.7.1.1.2 Transition timeline with key milestones.
5.7.1.1.3 Procedural manuals/guidelines.
5.7.1.1.4 Templates used in day-to-day operations.
5.7.1.1.5 Itemized list of additional equipment to be provided.
5.7.1.1.6 Process for transfer of on-hand inventory, if applicable.
Process for transfer of GFE/Recoverall inventory
5.7.1.1.7 Transition checklist.
5.7.1.1.8 Signed turnover agreements, if applicable.
5.7.1.1.9 System design plan.
5.7.1.1.10 Network architecture plan.

DELIVERABLE:

A. Phase-Out Transition Plan

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

6.1.1 ONE-VA TECHNICAL REFERENCE MODEL

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.

6.1.2 FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM)

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are Personal Identity Verification (PIV) card-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 comply with the VA Identity, Credential, and Access Management policies and guidelines set forth in the VA Handbook 6510 and align with the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance v2.0.

The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, 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 PIV card and/or Common Access Card (CAC), as determined by the business need.

The Contractor shall ensure all Contractor delivered applications and systems conform to the specific Identity and Access Management PIV requirements set forth in the Office of Management and Budget (OMB) Memoranda M-04-04, M-05-24, M-11-11, and NIST Federal Information Processing Standard (FIPS) 201-2. OMB Memoranda M-04-04, M-05-24, and M-11-11 can be found at: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy

04/m04-04.pdf, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-24.pdf, and https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf respectively. Contractor delivered applications and systems shall be on the FIPS 201-2 Approved Product List (APL). If the Contractor delivered application and system is not on the APL, the Contractor shall be responsible for taking the application and system through the FIPS 201 Evaluation Program.

The Contractor shall ensure all Contractor delivered applications and systems support:

1. Automated provisioning and are able to use enterprise provisioning service.
2. Interfacing with VA's Master Veteran Index (MVI) to provision identity attributes, if the solution relies on VA user identities. MVI is the authoritative source for VA user identity data.
3. The VA defined unique identity (Secure Identifier [SEC ID] / Integrated Control Number [ICN]).
4. Multiple authenticators for a given identity and authenticators at every Authenticator Assurance Level (AAL) appropriate for the solution.
5. Identity proofing for each Identity Assurance Level (IAL) appropriate for the solution.
6. Federation for each Federation Assurance Level (FAL) appropriate for the solution, if applicable.
7. Two-factor authentication (2FA) through an applicable design pattern as outlined in VA Enterprise Design Patterns.
8. A Security Assertion Markup Language (SAML) implementation if the solution relies on assertion based authentication. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST SP 800-63-3 guidelines.
9. Authentication/account binding based on trusted Hypertext Transfer Protocol (HTTP) headers if the solution relies on Trust based authentication.
10. Role Based Access Control.
11. Auditing and reporting capabilities.
12. Compliance with VAIQ# 7712300 Mandate to meet PIV requirements for new and existing systems. https://www.voa.va.gov/DocumentView.aspx?DocumentID=4846

The required Assurance Levels for this specific effort are Identity Assurance Level 3, Authenticator Assurance Level 3, and Federation Assurance Level 3.

6.1.3 TRUSTED INTERNET CONNECTION (TIC)

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/f

y2008/m08-05.pdf), M08-23 mandating Domain Name System Security (NSSEC) (https://obamawhitehouse.archives.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://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf.

6.1.4 STANDARD COMPUTER CONFIGURATION

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 365 ProPlus and Windows 10. However, Office 365 ProPlus and Windows 10 are not the VA standard yet and are currently approved for limited use during their rollout, we are in-process of this rollout and making them the standard by OI&T. Upon the release approval of Office 365 ProPlus and Windows 10 individually as the VA standard, Office 365 ProPlus and Windows 10 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 with switches for silent and unattended installation 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) and Defense Information Systems Agency (DISA) Secure Technical Implementation Guide (STIG) specific to the particular client operating system being used.

6.1.5 VETERAN FOCUSED INTEGRATION PROCESS (VIP)

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

6.1.6 PROCESS ASSETT LIBRARY (PAL)

The Contractor shall utilize PAL, the OI&T-wide process management tool that assists in the execution of an IT project (including adherence to VIP standards). PAL serves as an authoritative and informative repository of searchable processes, activities or tasks, roles, artifacts, tools and applicable standards or guides to assist project teams in facilitating their VIP compliant work.

6.2 SECURITY AND PRIVACY REQUIREMENTS

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.1	☒	☐	☐
5.2	☐	☒	☐
5.3	☐	☒	☐
5.4	☒	☐	☐
5.5	☐	☒	☐
	☐	☐	☐

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

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
b. 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 PAL template artifact. 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.

c. The Contractor should coordinate with the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized. The Contractor shall bring their completed Security and Investigations Center (SIC) Fingerprint request form with them (see paragraph d.4. below) when getting fingerprints taken.
d. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
    1) Optional Form 306
    2) Self-Certification of Continuous Service
    3) VA Form 0710
    4) Completed SIC Fingerprint Request Form
e. 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).
f. 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 e-QIP).
g. 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.
h. 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), completed training delineated in VA Handbook 6500.6 (Appendix C, Section 9), signed "Contractor Rules of Behavior", and with a valid, operational PIV credential for PIV-only logical access to VA's network. A PIV card credential can be issued once your SAC has been favorably adjudicated and your background investigation has been scheduled by OPM. 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 OPM.

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

Deliverable:

A. Contractor Staff Roster

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

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

6.4 PERFORMANCE METRICS

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

Performance Objective	Performance Standard	Acceptable Levels of Performance
A. 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
B. 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
C. Cost & Staffing	1. Currency of expertise and staffing levels appropriate 2. Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
D. 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. A Performance Based Service Assessment will be used by the COR in accordance with the QASP to assess Contractor performance.

6.5 FACILITY/RESOURCE PROVISIONS

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

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

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

This remote access may provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, PAL, 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.

6.6 GOVERNMENT FURNISHED PROPERTY

The Government has determined that remote access solutions involving Citrix Access Gateway (CAG) have proven to be an unsatisfactory access method to complete the tasks on this specific TO. The Government also understands that GFE is limited to Contractors requiring direct access to the network to: access development environments; install, configure and run TRM-approved software and tools (e.g., Oracle, Fortify, Eclipse, SoapUI, WebLogic, LoadRunner, etc.); upload/download/ manipulate code, run scripts, apply patches, etc.; configure and change system settings; check logs, troubleshoot/debug, and test/QA.

Based on the Government assessment of remote access solutions and the requirements of this TO, the Government estimates that the following GFE will be required by this TO:

1. **20** of standard laptops
2. **20** of developer-grade laptops

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 TO as necessary and any VA installation required for these IT accessories shall be coordinated with the COR.

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

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

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

Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices

are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, unless the connection uses FIPS 140-2 (or its successor) validated encryption, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COR, CO, the PM, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

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

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

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

A2.0 VA Enterprise Architecture Compliance

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

A2.1. VA Internet and Intranet Standards

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

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

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

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

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

A3.1. Section 508 – Electronic and Information Technology (EIT) Standards

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

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

A3.2. Equivalent Facilitation

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

A3.3. Compatibility with Assistive Technology

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

A3.4. Acceptance and Acceptance Testing

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

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

Automated test tools and manual techniques are used in the VA Section 508 compliance assessment.

Deliverables:

A. Final Section 508 Compliance Test Results

A4.0 Physical Security & Safety Requirements:

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

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

to protect persons and property from injury or damage during the performance of this contract.

A5.0 Confidentiality and Non-Disclosure

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

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

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA CO will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA CO for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA CO.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other

than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.

6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
    a. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
    b. Controlled access to system and security software and documentation.
    c. Recording, monitoring, and control of passwords and privileges.
    d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
    e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
    f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
    g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
    h. Contractor does not require access to classified data.
8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
9. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

A6.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13693, “Planning for Federal Sustainability in the Next Decade”, dated March 19, 2015; Executive Order 13221, “Energy-Efficient Standby Power Devices,” dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, Federal Energy Management Program (FEMP) designated, low

standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

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

1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).

2. Provide/use the purchasing specifications listed for FEMP designated products at https://www4.eere.energy.gov/femp/requirements/laws_and_requirements/energy_star_and_femp_designated_products_procurement_requirements . The Contractor shall use the low standby power products specified at http://energy.gov/eere/femp/low-standby-power-products.

3. Provide/use EPEAT registered products as specified at www.epeat.net. At a minimum, the Contractor shall acquire EPEAT® Bronze registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified product lists. The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists.

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

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

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

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

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

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

B1. GENERAL

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

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

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

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

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

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates (e.g. Business Associate Agreement, Section 3G), the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

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

B3. VA INFORMATION CUSTODIAL LANGUAGE

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

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

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

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

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

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

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.05, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

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

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

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

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

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

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

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

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

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

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

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

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

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

7. The Contractor/Subcontractor agrees to:

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

i. The Systems of Records (SOR); and

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

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

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

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

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

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

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

9. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as "Systems"), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hot fixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

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

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

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

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

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

be in accordance with the TIC Reference Architecture and reviewed and approved by VA prior to implementation. For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP).

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

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

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

e. The Contractor/Subcontractor must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The Government reserves the right to conduct such an assessment using Government personnel or another

Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

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

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

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

1) Vendor must accept the system without the drive;

2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or

3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;

a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and

b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.

c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

B6. SECURITY INCIDENT INVESTIGATION

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

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

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

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

B7. 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.

B8. TRAINING

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

1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the Information Security Rules of Behavior, updated version located at https://www.voa.va.gov/DocumentView.aspx?DocumentID=4848, relating to access to VA information and information systems;

2) Successfully complete the VA Privacy and Information Security Awareness and Rules of Behavior course (TMS #10176) and complete this required privacy and information security training annually;

3) 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.]

b. The Contractor shall provide to the CO and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 2 days of the initiation of the contract and annually thereafter, as required.

c. 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.