PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS (VA)
Veterans Health Administration (VHA)
Chief Business Office (CBO)

Veterans Point of Service (VPS)
Performance Management and Control

Date: December 16, 2015
PWS Version Number: 8.0

Contents

1.0 BACKGROUND

VHA evaluates process and technology improvements to improve clinical, administrative, and other services. VPS devices enable Veterans to make better use of their wait time at VA locations to update important information, filling out clinical questionnaires, reviewing medications and allergy updates, and providing important information to their care providers. VPS has completed national deployment of 4,508 freestanding, 540 desktop, and 331 wall mounted devices to the 160 Veteran Affairs Medical Centers (VAMCs) and their Community Based Outpatient Clinics (CBOCs). However, not all post-deployment activities have been completed.

Performance Management And Control (PM&C) provides the tools and services to monitor and improve VetLink performance across the VA Healthcare system today and as the VetLink product functionality expands. PM&C begins after the initial deployment of a VetLink system in a VAMC. There are many factors unique to this stage of a VetLink deployment in the VA. A typical VetLink deployment modifies the workflows of potentially hundreds of VA employees, and thousands of Veteran patients within each facility. Configuration, training, hardware placement, local workflows/policies, and experience levels of the administrators and end users can all contribute to performance below expected levels. PM&C engages with sites after activation and provides subject matter expert (SME) support to help site leads develop the experience and expertise to manage VetLink system performance. The first on-site PM&C visit occurs two weeks after initial activation and has a strong emphasis on evaluating the effectiveness of configuration, and providing desk side coaching for VA staff as needed.

Ninety days after VetLink activation the collection and analysis of performance data is initiated in order to quantify site performance. VetLink kiosks consist of groups with a common configuration, therefore any change that will affect performance must be done at the kiosk group level; in addition, performance data is collected, analyzed and corrected at the kiosk group level. In order to troubleshoot VetLink performance issues for a particular VAMC, the analyst must look at the performance of each kiosk group to isolate the problem.

A formal, onsite kick-off meeting and performance audit occur shortly after the first 90 days of data analysis. Prior to the meeting, a site evaluation plan draft is prepared based on performance data and configuration analysis. The report contains data for each current key performance metric and identifies specific kiosk groups (check-in areas) that need further investigation. The PM&C team presents findings and collaborates with the site lead to develop action items and a plan to fix the root causes of underperformance in each area in order to improve the overall performance of the VetLink system.

The onsite meeting includes a walk-through of all deployed kiosks to evaluate kiosk placement and signage. Staff users are interviewed in order to gauge how effective VetLink is integrated with the patient workflow, and to identify any problems affecting patient and staff users. The walk-through may also identify areas in need of additional

VetLink hardware, or new/advanced functionality that must be activated. The results and recommendations are shared with the site lead.

After the onsite meeting, and for the next 9-12 months, THE PM&C TEAM works closely with the site lead to improve performance and provide monthly reports and analysis to continue to support the site. During this period, the site should become more proficient at managing all aspects of the system independently.

Because the PM&C team maintains a relationship with each site and provides the subject matter expertise on VetLink system configuration and usage, it is in a unique position to consult with site leads to determine and prioritize the activation of new functionalities. VPS releases a new version of VetLink approximately every six months. New versions typically include enhancements to existing functionality and the introduction of new functionality. Existing VetLink servers are updated with the new release after the user acceptance testing, pilot testing, and operational readiness review process and approval for national release are given. These updates occur in rapid succession, ensuring that all VetLink deployments are running the same, nationally-approved VetLink version. New functionality is then available to all sites, but only configured and activated at a few pilot sites. At this point the VA has invested in the development of substantial new functionality but is not yet realizing the benefits of that investment.

2.0 APPLICABLE DOCUMENTS

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

1. 44 U.S.C. § 3541, “Federal Information Security Management Act (FISMA) of 2002”
2. Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements For Cryptographic Modules”
3. FIPS Pub 201-2, “Personal Identity Verification of Federal Employees and Contractors,” August 2013
4. 10 U.S.C. § 2224, "Defense Information Assurance Program"
5. Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Development (CMMI-DEV), Version 1.3 November 2010; and Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Acquisition (CMMI-ACQ), Version 1.3 November 2010
6. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
7. 42 U.S.C. § 2000d “Title VI of the Civil Rights Act of 1964”
8. VA Directive 0710, “Personnel Suitability and Security Program,” June 4, 2010, http://www1.va.gov/vapubs/
9. VA Handbook 0710, Personnel Suitability and Security Program, September 10, 2004, http://www1.va.gov/vapubs/
10. VA Directive and Handbook 6102, “Internet/Intranet Services,” July 15, 2008

11. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
12. Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources,” November 28, 2000
13. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
14. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
15. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
16. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
17. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, , 2012
18. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” September 20, 2012
19. VA Handbook 6500.1, “Electronic Media Sanitization,” March 22, 2010
20. VA Handbook 6500.2, “Management of Data Breaches Involving Sensitive Personal Information (SPI)”, January 6, 2012
21. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring Of VA Information Systems,” February 3, 2014
22. VA Handbook, 6500.5, “Incorporating Security and Privacy in System Development Lifecycle” March 22, 2010
23. VA Handbook 6500.6, “Contract Security,” March 12, 2010
24. Project Management Accountability System (PMAS) portal (reference https://www.voa.va.gov/pmas/)
25. OI&T ProPath Process Methodology (reference https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=27) NOTE: In the event of a conflict, OI&T ProPath takes precedence over other processes or methodologies.
26. Technical Reference Model (TRM) (reference at http://www.va.gov/trm/TRMHomePage.asp)
27. VA Technology Strategies
    a. Architectural Strategy Design (ASD) and the Design Pattern – Service-Oriented Architecture (SOA) Design Patterns - http://www.techstrategies.oit.va.gov/docs_design_patterns_soa.asp
    b. Authentication, Authorization, and Audit Design Patterns - http://www.techstrategies.oit.va.gov/docs_design_patterns_aaa.asp
28. Open Source Electronic Health Record Agent (OSEHRA), www.osehra.org
29. SMART Platform technology at http://smartplatforms.org
30. National Institute Standards and Technology (NIST) Special Publications (SP)
31. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008
32. VA Directive 6300, Records and Information Management, February 26, 2009

33. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
34. OMB Memorandum, “Transition to IPv6”, September 28, 2010
35. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, February 17, 2011
36. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 20, 2014
37. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
38. 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
39. 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
40. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
41. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
42. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
43. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
44. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
45. Draft NIST Special Publication 800-157, Guidelines for Derived PIV Credentials, March 2014
46. NIST Special Publication 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
47. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
48. 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)
49. VA Memorandum, VAIQ # 7011145, VA Identity Management Policy, June 28, 2010 (reference Enterprise Architecture Section, PIV/IAM (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
50. 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)
51. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, October 1, 2013
52. OMB Memorandum M-08-05, “Implementation of Trusted Internet Connections (TIC), November 20, 2007

53. OMB Memorandum M-08-23, Securing the Federal Government's Domain Name System Infrastructure, August 22, 2008
54. 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)
55. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
56. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
57. Executive Order 13514, "Federal Leadership in Environmental, Energy, and Economic Performance," October 5, 2009
58. Executive Order 13423, "Strengthening Federal Environmental, Energy, and Transportation Management," January 24, 2007
59. Executive Order 13221, "Energy-Efficient Standby Power Devices," August 2, 2001
60. VA Directive 0058, "VA Green Purchasing Program", July 19, 2013
61. VA Handbook 0058, "VA Green Purchasing Program", July 19, 2013
62. CTS Note #1: A VA Executive's Guide to Databases (December 2013)
63. http://www.techstrategies.oit.va.gov/TECHSTRATEGIES/docs/CTSNotes/CTSNoteDec2013.pdf
64. CTS Note #2: A VA Executive's Guide to Virtualization (January 2014)
65. http://www.techstrategies.oit.va.gov/TECHSTRATEGIES/docs/CTSNotes/CTSNoteJan2014.pdf
66. CTS Note #3: A VA Executive's Guide to Web Service Layers (February 2014)
67. http://www.techstrategies.oit.va.gov/TECHSTRATEGIES/docs/CTSNotes/CTSNoteJan2014.pdf
68. VA Handbook 6500.6, "Contract Security," March 12, 2010
69. VA Directive 6502, VA Enterprise Privacy Program
70. VA Directive 6502.3, Web Page Privacy Policy
71. VA Directive 6513, Secure External Connections
72. VA Directive 6515, Use of Web-Based Collaboration Technologies
73. VA Directive 6517, Cloud Computing Services

3.0 SCOPE OF WORK

The Contractor shall assist VA with the Performance Management and Control activities for VetLink sites. The Contractor shall develop performance management tools, such as dashboards, collect data, perform analysis, and provide monthly reports and weekly reports as needed. The Contractor shall provide monthly reports for VetLink sites as part of its support of the VPS PM and other VA stakeholders. The Contractor shall support the 90 day post deployment visits to the remaining 84 VetLink sites. The Contractor shall support the release of new VetLink functionality as well.

The Contractor shall have the capability to provide management and oversight of the performance management and control activities, perform data collection, and perform analysis as requested. The Contractor shall have at least one year of experience providing training and performance improvement recommendations to a nation-wide information system.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance shall be 12 months from the date of award, with one, 6-month option period to be exercised at the Government's discretion.

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

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

Under current definitions, four are set by date:

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

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

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

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

4.2 PLACE OF PERFORMANCE

Tasks under this PWS shall take place primarily at the Contractor's facility. As needed and with approval of the COR, Contractor staff may visit VA locations (Appendix X) to provide the support defined in the tasks below.

4.3 TRAVEL

The Government anticipates travel under this effort to perform the tasks associated with the effort, as well as to attend program-related meetings or conferences through the

period of performance. Include all estimated travel costs in your firm-fixed price line items. These costs will not be directly reimbursed by the Government.

The total estimated number of trips in support of the program related meetings for this effort is175 trips to VA locations with VetLink kiosks (estimated 20 meetings/conferences and 155 site trips). Anticipated duration of the trips is four days.

Travel shall be in accordance with the Federal Travel Regulations (FTR).

4.4 GOVERNMENT FURNISHED PROPERTY

No government furnished property, also known as government furnished equipment (GFE) will be required for this contract.

All Contractor personnel shall be provided access to VA Citrix Remote Access/CAG and contractors with GFE shall be provided VPN access. The Contractor will be provided VA tools such as Microsoft Lync, VA CRM's pages on Microsoft SharePoint, and other VA collaboration tools in order to complete tasks successfully.

The following Government Furnished Information (GFI) will be provided to the Contractor upon award:

1. VPS 90 Day Site Visit Training Materials
2. VPS Existing Post Deployment Training Plan

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following activities listed in the sections below. The Contractor shall be responsible for providing the deliverables listed in the sections below, and all the services providing a successful outcome. These documents shall be created using Microsoft Word, Microsoft Excel, Microsoft PowerPoint, and/or Microsoft Project. All draft documents shall be delivered in one of these formats. All final documents shall be delivered in one of these formats as well as PDF. Additionally, all shared documents shall also be in one of the above formats. The VA will have 10 days to review and provide feedback to the Contractor on all deliverables. The Contractor will have five (5) days to provide the final deliverable.

The VA assumes the Contractor to use agile development and fully support the software development lifecycle (SDLC). The Contractor shall deliver and support all artifacts associated with technical and functional components necessary for the project to meet ProPath process requirements and ensure VA Project Management Accountability System (PMAS) compliance. PMAS describes a schedule of incremental deliveries of useable capabilities every six months (http://vaww.oed.oit.va.gov/process/propath/).

The Contractor shall develop deliverable artifacts that are consistent with PMAS and ProPath templates. The Contractor shall include only the content and artifacts that have been updated or developed in the target increment in deliverable packages. When no change to a package component has occurred during an increment, unrelated or

unchanged artifacts will not be included in the associated delivery packages. The Contractor shall provide a revision history with track changes on to allow for easy visibility of changes between package deliverables.

5.1 PROJECT MANAGEMENT

5.1.1 PROJECT MANAGEMENT PLAN

The Contractor shall deliver a Project Management Plan (PMP) that lays out the Contractor's approach, timeline and tools to be used in execution of this Task Order effort. The PMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks, and resource support. The PMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The initial baseline PMP shall be concurred upon and updated monthly thereafter. The Contractor shall update and maintain the VA PM approved PMP throughout the period of performance.

The Contractor shall:

1) Conduct weekly communication with the VA PM, additional VPS PMs as dependent projects require, additional Contractors as appropriate and keep the COR abreast of associated activities and projects related to the Cloud;
2) Utilize project metrics to track, analyze and advise on task progress, communicate findings to the VA PM and COR, and ensure appropriate focus on critical attention areas;
3) Provide administrative, managerial and financial inputs to the VA PM on all reporting efforts including cost and schedule, status, dashboard reporting, and data call response reporting;
4) Provide a Fully Resourced Schedule for 90-day post deployment. This will include the proposed order of travel for the 90-day post deployment meetings, and who will be attending for each site;
5) Provide and maintain contractor Staff Roster which shall include, but not be limited to, each staff member's name, contact address, contact telephone number and email address;
6) Participate in the VPS project management and control activities including:
    a. Completing risk identification log when risks are identified; and
    b. Entering time and progress against activities for the VPS integrated master schedule

The Contractor shall provide an Integrated Master Schedule (IMS) in Microsoft Word.

Deliverables:

A. Project Management Plan
B. Fully resourced schedule (90 day post deployment)
C. Staff Roster
D. Risk Identification Log

5.1.2 REPORTING REQUIREMENTS

The Contractor shall deliver Bi-Weekly (every two weeks) Task Order Status Reports. These reports shall provide accurate, timely, and complete project information supporting the task order. The Bi-Weekly Task Order Status Report shall include the following data elements:

a) Project Name and <Contract/Task Order> Name
b) Overview and description of the <Contract/Task Order>
c) Overall high level assessment of <Contract/Task Order> progress
d) All work in-progress and completed during the reporting period
e) Identification of any <Contract/Task Order> related issues uncovered during the reporting period and especially highlight those areas with a high probability of impacting schedule, cost or performance goals and their likely impact on schedule, cost, or performance goals
f) Explanations for any unresolved issues, including possible solutions and any actions required of the Government and/or Contractor to resolve or mitigate any identified issue, including a plan and timeframe for resolution
g) Status on previously identified issues, actions taken to mitigate the situation and/or progress made in rectifying the situation.
h) Work planned for the subsequent four reporting periods, when applicable
i) Current <Contract/Task Order> schedule overlaid on original <Contract/Task Order> schedule showing any delays or advancement in schedule
j) Provide summary of all 90-day post-deployment trips, and notes taken from the 90-day leadership discussions, lessons learned from each site, areas of improvement, and training evaluations from each site.
k) Summary of the cord management work performed during the period, and the remaining cord management work to complete.
l) Workforce staffing data showing all Contractor personnel performing on the effort during the current reporting period. Each Bi-Weekly Task Order Status Report shall also identify any changes in staffing identifying each person who was added to the contract or removed from the contract.
m) Original schedule of deliverables and the corresponding deliverables made during the current reporting period.

These reports shall not be the only means of communication between the contractor, COR and the Program/Project Manager to advise of performance/schedule issues and to develop strategies for addressing the issues. The Contractor shall continuously monitor performance and report any deviation from previous Bi-Weekly Task Order Status Report to the COR and Program/Project Manager during routine, regular communications.

Deliverables:

A. Bi-Weekly Status Report

5.1.3 TECHNICAL KICK OFF MEETING

The Contractor shall provide a kick-off meeting for the government within five days of award. The Contractor shall present, for review and approval by the Government, the details of the intended approach, work plan, and project schedule for each effort. The Contractor shall specify dates, location (can be virtual) andagenda (shall be provided to all attendees at least three days prior to the meeting The Contractor shall invite the CO, VA COR, VA Project Manager (PM), and VPS Program Director.
The Contractor shall also perform a kickoff meeting for the work in the Optional Task(s).

Deliverables:

A. Kickoff Meeting
B. Agenda for Kickoff Meeting

5.1.4 PRIVACY TRAINING

The Contractor shall submit status of VA Privacy and Information Security Awareness training for all individuals engaged on the task. The status reporting shall identify; a single Contractor Security POC, the names of all personnel engaged on the task, their initial training date for VA Privacy and Information Security training, and their next required training date. This information shall be submitted as part of the Bi-Weekly PD Status Report.

The Contractor shall submit VA Privacy and Information Security training certificates in accordance with Section 9, Training, from Appendix C of the VA Handbook 6500.6, “Contract Security”.

Deliverables:

A. VA Privacy and Information Security Training Certificates

5.2 PERFORMANCE MANAGEMENT AND CONTROL

The Contractor shall assist VA with the PM&C activities for VetLink sites. The Contractor shall utilize its Business Intelligence tool to collect data, perform analysis, provide visual representations (dashboards) of the analysis, and provide monthly and weekly reports. The Contractor shall provide monthly reports for VetLink sites as part of its support of the VPS Project Manager (PM) and other VA stakeholders. The Contractor shall support the 90 day post deployment visits to at least 60 of the remaining 84 VetLink sites and shall perform site evaluations and improvement discussions as well as perform additional kiosk usage training for at least these sites. The Contractor shall support these sites and the other sites requiring additional education and support to mature to sustainment level. The Contractor shall support the release of new VetLink functionality as well.

5.2.1 PERFORMANCE MANAGEMENT AND CONTROL REQUIREMENTS

The purpose of PM&C is to assist VetLink sites with managing their performance from new user to self-sustaining VetLink experts; provide up-to-date dashboard views of individual VAMCs, VISNs, and aggregated national VetLink performance for VPS management; and assist them to maturity; and maintain the configuration description

and functionality access for all VetLink sites (such as which ones are using BeneTravel and which ones are not).

A key factor of the 90-day post deployment support is the collection, analysis, and presentation of VetLink usage at all VA sites to compare the newly deployed sites to all others. VPS requires PM&C that covers:

- Pro-active performance management and control of individual VetLink deployments
- Measure system-wide VetLink performance against key, national metric targets
    1. 25% Usage in 1st Year
    2. 35% Usage in 2nd Year
    3. 40% Usage in 3rd Year
- Provide SME expertise support to identify and resolve performance issues at all VetLink sites
- Maintain the Contractor's existing database to hold the metric data
- Utilize a Business Intelligence Tool to extract metric data from the kiosk and provide a report of the data.
- Report on performance data at the different levels
- Create dashboards to display the trends
- Provide training

The following metrics shall be collected by the Contractor:

- **Utilization data (monthly):** Total number of appointments checked in on kiosk out of total number of appointments available
- **Kiosk Interactions:** Number of kiosk uses that resulted in kiosk check-in or manual assisted check-in
- **Patient updates**: Total number of patient demographic updates made on kiosk, audited by staff
- **Satisfaction Survey Results**: VISN average of patients who responded yes to question. "Was kiosk easy to use". (Survey and questionnaire results)
- **Insurance Opportunity**: The total number of patients that indicated, on kiosk that their current insurance has changed

5.2.2 COLLECT, ANALYZE, AND REPORT

The Contractor shall collect performance (% Usage) from all VetLink sites. The Contractor shall analyze the data, troubleshoot performance problems, and generate the reports detailed below.

The Contractor shall use its automated data collection tool that on a weekly basis collects and aggregates the performance data for the metrics defined above in Section 5.2.1 from all VetLink sites and places that data into the existing performance data database. This automated collection tool shall also have a feature that allows the Government to collect data manually as required. The Contractor shall ensure that the data collection process is completed successfully at all sites weekly so that data

analysis can be performed each week by including success into the Monthly Program Review (MPR). The Contractor shall ensure all performance data is available to view on the dashboards (5.2.3) by data analysts, performance analysts and VPS PMO users.

The Contractor shall:

- Collect data from all VA sites with kiosks weekly and manually as required
- Verify in the MPR that all required performance data was collected from all VetLink sites
- Aggregate data into the performance data database

Once the performance data has been collected weekly, the Contractor shall perform an evaluation of each performance metric. The Contractor shall analyze adoption, success rates, and key metrics as compared to VPS-defined performance targets (defined in 5.2.1 above) for each metric to identify issues. The Contractor shall perform weekly analysis of all metric data from all VetLink sites and identify all performance issues and potential resolutions to identify replicable reasons. The Contractor shall perform trouble shooting for all identified performance issues at all VetLink sites. For VetLink sites that are having performance issues, the Contractor shall work with VetLink site leads to provide insight and advice on how to improve performance. The Contractor shall document and communicate all issues and resolutions to the site leads and to VPS PM.

The Contractor shall provide monthly site-performance reports (Site, VAMCs, VISNs, and National) customized for each deployed VetLink site. The monthly site-performance report shall contain the cumulative work output of data collection, analysis, troubleshooting, and collaboration. The monthly report shall be delivered to each site lead (attached document: VPS Site Leads list.xls), VPS PM, and the COR at regular monthly intervals. The VPS PM shall periodically evaluate the monthly report template and make adjustments as needed to improve the effectiveness of the reports.

The monthly site performance report shall include:

A. Current phase of site maturity
B. Executive Summary
C. Performance Concerns
D. Recommended Action Items
E. Overall site metrics
F. Metrics by Clinic Area (kiosk group)
G. Hardware & Configuration requests
H. Major Support Issues

The VAMC monthly performance report shall include:

I. Executive Summary
J. Current phase of each sites maturity
K. Performance Concerns – site specific and VAMC-wide
L. Recommended Action Items by site
M. Metrics by Site and kiosks group
N. Hardware & Configuration requests
O. Major Support Issues

The VISN monthly performance report shall include:

P. Executive Summary
Q. Current phase of each sites maturity
R. Performance Concerns – site specific and VISN-wide
S. Recommended Action Items by site
T. Metrics by Site and kiosks group
U. Hardware & Configuration requests
V. Major Support Issues

The National monthly performance report shall include:

W. Executive Summary
X. Current performance levels for each site
Y. Current maturity levels for each site
Z. Key performance metrics by 161 VAMCs
AA. Performance Concerns
BB. Recommended Action Items by site
CC. Hardware & Configuration requests by 161 VAMCs
DD. Major Support Issues

The Contractor shall provide the first monthly report covering the first and second month and monthly from there on out through the life of the contract.

Deliverables:

A. VetLink Site Monthly Performance Report
B. VetLink VAMC Monthly Performance Report
C. VetLink VISN Monthly Performance Report
D. VetLink National Monthly Performance Report

5.2.3 DASHBOARDS DEVELOPMENT

The Contractor shall develop interactive dashboards that dynamically generate summarized performance metrics in graphical form, and identify and isolate VetLink performance strengths or weaknesses configurable to the different site levels (VetLink sites, VAMCs, VISNs, and National levels).

The Contractor shall develop the dashboards based upon the performance data reports developed in Section 5.2.2. The dashboards need to be dynamic, real-time, interactive and built to be viewable from a VA approved browser. The Contractor shall also provide dashboards to track new feature activation and usage at each VAMC. As new features are released, benefits are not realized until the feature is activated at medical centers and used by patients. These dashboards shall track the adoption of newly-deployed features for each release, at each site, allowing VPS leadership to quantify the current activation and usage of each feature independently.

The Contractor shall provide mockups of all dashboards for VA PM Approval prior to implementation.

Deliverables:

A. VetLink Dashboard Mockups

5.2.4 VETLINK PRE-RELEASE DOCUMENTATION

The Contractor shall document pre-release information for all software applications via a Microsoft Excel Workbook (the file must be created and maintained in Excel). The Contractor shall work with the existing release contractor to acquire the required release information to perform this task. It is anticipated for there to be one (1) release per quarter. The Contractor shall create a workbook that includes the name of the releases, the functionality, whether the release is new or an enhancement, release date, and integration with identified VistA applications. The pre-release documentation will ensure that all facilities are aware of the new updates and the potential impact to current business processes once the sites have activated the kiosks.

Deliverables:

A. VetLink Pre-Release Documentation

5.2.5 90-DAY VISIT SUPPORT

The Contractor shall perform a 90-day site visit for the at least 60 of the 84 VetLink sites. The Contractor shall develop a site visit plan that includes analyzing time required for data collection, aligning visits with sites that are located near each other, and/or other critical factors. The Contractor shall deliver the Site Visit Plan to the VA PM for approval.

Once the plan for the visits has been approved for the VPS PM, the Contractor shall collect and analyze performance data in order to quantify each site's performance. Performance data must be collected and analyzed at the kiosk group level. The Contractor shall review and analyze the performance detail at the kiosk group level to identify issues and concerns. In advance of the 90-day visit, the Contractor shall create a Site Evaluation Plan based on the performance data and configuration analysis that contains performance data for each current key performance metric and identifies specific kiosk groups that need further systemic studies

At the 90-day visit, the Contractor shall participate in a technical exchange meeting to present the initial findings from the draft action plan. The Contractor shall document the root causes and action items to revise the Site Evaluation Action Plan. The Contractor shall document findings on the placement effectiveness, training needs, hardware needs, and new functionality for activation.

At the end of each 90 day visit, the Contractor shall participate in an exit interview with Site Leadership. The Contractor shall provide the VA PM and VA COR copies of the 90 leadership presentations for review and approval 2 weeks prior to the site visit.

Deliverables:

A. Site Visit Plan

B. Site Visit Schedule
C. Site Visit Draft Action Evaluation Plan
D. Site Visit Final Action Evaluation Plan
E. 90-Day Leadership Discussion Presentation

5.2.6 VPS TRAINING

The Contractor shall work with the VA PM and the Site Lead to determine the type of training required for the 90-day site visit and then execute the approve training for at least 60 of the 84 VetLink sites. The training materials will be provided by the Government upon Contract Award. VPS national deployment ended in November 2014; however, not all VA locations have received 90-day post-deployment training. 90-day post-deployment training reinforces the original training and provides initial training to staff unable to attend initial training, and assists in the full operation status of VetLink at each VA location. This 90 day visit training consists of onsite meetings with leadership and one-on-one training for those users who require it.

The Contractor shall also support the VA sites whose Performance Metrics (i.e. kiosks interactions) do not meet the VPS national standards. The Contractor shall discuss with the site leads resolutions to those metrics that do not meet the national standards. The Contractor shall work with the VA to ensure required training, access to reports and software upgrades are available to the site and provide updates to the VA, as part of the bi-weekly report.

The Contractor shall also revise the VPS approved existing post-deployment training plan detailing how post-deployment support shall be coordinated with the VPS designated personnel. Post-deployment training includes training related to leadership oversight and transitioning of roles from the Contractor to the local staff. The Contractor shall develop training materials, establish evaluation techniques, and create a deployment scorecard. The training plan shall be updated in MS Word and be supported with the Integrated Master Schedule (IMS). The Contractor shall outline learning approaches that can be applied to on-the-job and sustainment of skills to support VA staff, so employees can continue to provide high quality services to Veterans. The plan shall include performance-based measures tied to clearly defined performance outcomes based on the use of the kiosks. The plan shall address designated position roles (i.e., Report Specialist, Application Administrator, System Administrator, and Associate).

The Contractor shall work with the VA PM and the VetLink Kiosk Site Lead to determine the type of training required when new functionality has been deployed. The Contractor may be required to provide configuration support and training for all VA facilities with VPS kiosks (over 160 VAMCs and 600 CBOCs). The Contractor shall schedule onsite training within 30 days of the request if the functionality already exists.

The Contractor shall schedule training for all new functionality 60 to 90 days after the release of the new functionality. This may be virtual or onsite depending on the sites needs and approval by VPS PM.

Deliverables:

A. Updated Post-Deployment Training Plan and Materials

5.2.7 NEW FUNCTIONALITY CONFIGURATION

The VPS Program creates new functionality of the VetLink program. The VA estimates two releases with new functionality, and four patches per year. These new releases usually contain new and sometimes complex functionalities requiring specific configuration of a site's VetLink. Additionally, sites may choose to turn-on previously turned-off functionality which also requires specific configuration and training. The Contractor shall provide configuration support for new functionality as well as for when sites turn-on existing functionality that was previously not utilized.

5.3 VETLINLK KIOSK THERMAL PAPER

The Contractor shall provide support for replacing thermal paper for all deployed kiosks through the Operations and Maintenance (O&M) Center. The O&M Center will send the help desk request to the Contractor to process as they are received. On average, VPS needs 48 cases of thermal paper replacement paper per month. A case includes 50 rolls of thermal paper. The Contractor shall purchase and inventory replacement kiosk thermal papers, ship paper to the existing Help Desk Contractor as required by the O&M help desk ticket, and track and manage inventory levels. The Contractor shall provide a monthly status report to the O&M Center for inclusion into their reports.

Deliverables:

A. Monthly Thermal Paper Status Report

5.4 NSOC REMEDIATION

The Contractor shall manufacture and/or obtain and supply the following to hardware upgrades to the VetLink kiosks to remediate physical access to ports on the kiosks for every kiosk purchased by the VA:

- Metal security bracket cover
- Tamper-resistant security screws
- Special driver to operate the security screws

Additionally, the Contractor shall customize, assemble, and package a hardware upgrade kit for every VA location – 161 primary VA locations, and 667 CBOCs. Each hardware package upgrade kit shall include:

- Kiosks I/O security bracket(s)
- Tamper-resistant security screws
- Driver bit for security screws (capable of fitting a standard ¼" multi-bit driver to be supplied by the VA)
- Installation instructions

The Contractor shall ship to the packages to the 161 primary VA locations for the VA to install on the VetLink kiosks. The shipment to the primary location will include the kits for the CBOCs associated with that location.

The Contractor shall provide the following packaged and shipped as described above: The Government shall provide the Contractor with a kiosk in order for them to measure, design and fabricate the kits.

Description	Quantity
Kiosk I/O Bracket – made from sheet metal, powder coated to match kiosk, molded to bend around kiosk head to prevent removal of cable bay door without proper tools. Also accommodates a standardized laptop cable lock, allowing desktop kiosks to be fastened to a fixed structure.	6,000
Bryce Penta-Plus Tamper-resistant security screws	24,000
Bryce Penta-Plus Tamper-resistant security driver bits for the security screws	2,000

The Contractor will have 90 days from award to purchase, draft instructions for connection off items, and ship items to the field. The NSOC remediation kits and styli not being shipped will be included in all new kiosk requests to the field.

5.5 VPS PMC OPTION PERIOD ONE

Option Period 1 shall have a six (6) month period of performance if exercised by the Government. For Option Period 1, the Contractor shall provide all of the support contained within Sections 5.1, 5.2, 5.3, 5.4, and related subsections.

The Contractor shall support the 90 day post deployment visits to no more than 24 of the remaining 84 VetLink sites. The Contractor shall perform the site evaluation and improvement discussions as well as perform additional kiosk usage training for no more than 24 of the remaining sites. The Contractor shall support these sites and the other sites requiring additional information and support to mature to sustainment level. The Contractor shall support the release of new VetLink functionality as well.

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (One-VA TRM). One-VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications.

One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. Architecture, Strategy, and Design (ASD) has overall responsibility for the One-VA TRM.

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

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

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

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

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

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

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

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

Position Sensitivity	**Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A)
Low / Tier 1	**Tier 1 / National Agency Check with Written Inquiries (NACI)** A Tier 1/NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.
Moderate / Tier 2	**Tier 2 / Moderate Background Investigation (MBI)** A Tier 2/MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree.
High / Tier 4	**Tier 4 / Background Investigation (BI)** A Tier 4/BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree.

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

	Position Sensitivity and Background Investigation Requirements		
Task Number	Tier1 / Low / NACI	Tier 2 / Moderate / MBI	Tier 4 / High / BI
5.1	☐	☒	☐
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. The Contractor shall bear the expense of obtaining background investigations.
c. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the ProPath template. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.

d. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
e. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
    1) For a Tier 1/Low Risk designation:
        a) OF-306
        b) DVA Memorandum – Electronic Fingerprints
    2) For Tier 2/Moderate or Tier 4/High Risk designation:
        a) OF-306

b) VA Form 0710
c) DVA Memorandum – Electronic Fingerprints

f. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
g. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via eQIP).
h. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
i. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or "Closed, No Issues" (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).
j. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
k. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.
l. Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

Deliverable:

A. Contractor Staff Roster

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

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

6.4 PERFORMANCE METRICS

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

#	Area	Description	Requirement
1	Progress	The Bi-Weekly Progress Report will provide information on how well the project is performing with respect to its approved schedule and period of performance. No Schedule slippage due to changing contractor personnel.	Must meet expected number of trips 100% of time.
2	Staffing	The Project Management Plan and Resource schedule will provide visibility into the contributions of staffing on project costs, schedule adherence and product quality in accordance with the submitted proposal	At least 95% of the proposed staffing, schedule and cost remain consistent with the original proposal
3	Quality	Provide reports free of spelling, grammatical, and math errors	95% of reports are accurate and free of mathematical, grammatical, and formatting errors
4	Timeliness	Provide reports and deliverables timely	100% of reports/deliverables are delivered on-time based on the project plan

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

6.5 FACILITY/RESOURCE PROVISIONS

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

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

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

6.6 GOVERNMENT FURNISHED PROPERTY

Not applicable

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

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

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

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

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

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

Not applicable

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: http://www.section508.gov and http://www.section508.gov/acquisition-regulations. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

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

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. Representation of Conformance

In order to be considered eligible for award, offerors must submit the Government Product Accessibility Template (GPAT) to verify Section 508 conformance of their products and/or services. The GPAT will be incorporated into the resulting contract.

A3.5. 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 a final/updated GPAT and 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 508 Compliance before delivery. The Contractor shall be able to demonstrate 508 Compliance upon delivery.

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

Deliverable:

A. Updated GPAT
B. 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 Contracting Officer will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA Contracting Officer for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA Contracting Officer.

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

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 13514, "Federal Leadership in Environmental, Energy, and Economic Performance," dated October 5, 2009; Executive Order 13423, "Strengthening Federal Environmental, Energy, and Transportation Management," dated January 24, 2007; Executive Order 13221, "Energy-Efficient Standby Power Devices," dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, 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 www.femp.energy.gov/procurement. 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 Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor's employ. The Contracting Officer must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

B3. VA INFORMATION CUSTODIAL LANGUAGE

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

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

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

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

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

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

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

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

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

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

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

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

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

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

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 Appendix D of VA Handbook 6500, *VA Information Security Program*). 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, *VA 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 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) 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, *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 (3), 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 contracting officer 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 reviewed and approved by VA prior to implementation.

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

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

d. The Contractor/Subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer 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 C&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 C&A would be necessary.

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

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

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

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

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

1) Vendor must accept the system without the drive;

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

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

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

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

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

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

B6. SECURITY INCIDENT INVESTIGATION

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

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

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

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

B7. LIQUIDATED DAMAGES FOR DATA BREACH

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

b. The Contractor/Subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other

unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

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

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

a) date of occurrence;

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

3) Number of individuals affected or potentially affected;

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

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

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

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

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

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

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

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

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

1) Notification;

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

B8. SECURITY CONTROLS COMPLIANCE TESTING

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

B9. TRAINING

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

1) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* course (TMS #10176) and complete this required privacy and security training annually; Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems.

2) Successfully complete any additional 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 contracting officer 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 contracting officer and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training and 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.