PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology (OI&T), Service Delivery and Engineering (SDE)
Enterprise Operations (EO)
Hines Information Technology Center (HITC)

Local Exchange Carrier (LEC) Services connecting to a Voice over Internet Protocol (VoIP) Telephone System

Date: 02/19/2015
TAC-15-20211
PWS Version Number: 3.0

Contents

1.0 BACKGROUND

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

HITC located at First Avenue North of 22nd Street, Building 215, Hines, IL 60141 requires telephone circuits from a local exchange carrier (LEC) company to provide voice communication services at this location. Services include Integrated Services Digital Network (ISDN), Primary Rate Interfaces (PRIs), Direct Inward Dialing (DID) two way, combination, inbound/outbound, and both-way, and Directory Listing service. In addition, the Contractor shall provide and install the hardware for PRI service to the demarcation point in the MDF room. This hardware is for the sole purpose of PRIs and is installed, configured and maintained by the Contractor. ISDN PRI service is required to replace the existing Centrex telephone service which consists of AT&T provided Alcatel Lightspan Centrex termination equipment at the customer location. The new telephone service delivered via Primary Rate Interface (PRI) circuits will interface to a VA owned new Voice over Internet Protocol (VoIP) Telephone system. The Contractor shall provide a seamless transition from the Centrex service to the PRI service

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&TProPath Process Methodology (reference https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=27)NOTE: In the event of a conflict, OI&TProPath takes precedence over other processes or methodologies.
26. Technical Reference Model (TRM) (reference athttp://www.va.gov/trm/TRMHomePage.asp)
27. National Institute Standards and Technology (NIST) Special Publications (SP)
28. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008

29. VA Directive 6300, Records and Information Management, February 26, 2009
30. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
31. OMB Memorandum, “Transition to IPv6”, September 28, 2010
32. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, February 17, 2011
33. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 20, 2014
34. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
35. OMB Memorandum 05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005
36. OMB memorandum M-11-11, “Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011
37. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
38. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
39. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
40. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
41. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
42. Draft NIST Special Publication 800-157, Guidelines for Derived PIV Credentials, March 2014
43. NIST Special Publication 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
44. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
45. VA Memorandum, VAIQ #7100147, Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12), April 29, 2011 (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
46. VA Memorandum, VAIQ # 7011145, VA Identity Management Policy, June 28, 2010 (reference Enterprise Architecture Section, PIV/IAM (referencehttps://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
47. IAM Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, PIV/IAM (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)

48. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, October 1, 2013
49. OMB Memorandum M-08-05, “Implementation of Trusted Internet Connections (TIC), November 20, 2007
50. OMB Memorandum M-08-23, Securing the Federal Government’s Domain Name System Infrastructure, August 22, 2008
51. VA Memorandum, VAIQ #7497987, Compliance – Electronic Product Environmental Assessment Tool (EPEAT) – IT Electronic Equipment, August 11, 2014 (reference Document Libraries, EPEAT/Green Purchasing Section,https://www.voa.va.gov/documentlistpublic.aspx?NodeID=552)
52. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
53. Section 104 of the Energy Policy Act of 2005,(Public Law 109–58), August 8, 2005
54. Executive Order 13514, “Federal Leadership in Environmental, Energy, and Economic Performance,” October 5, 2009
55. Executive Order 13423, “Strengthening Federal Environmental, Energy, and Transportation Management,” January 24, 2007
56. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
57. VA Directive 0058, “VA Green Purchasing Program”, July 19, 2013
58. VA Handbook 0058, “VA Green Purchasing Program”, July 19, 2013

3.0 SCOPE OF WORK

The Contractor shall provide all hardware, installation, configuration and repairs required to supply ISDN, PRI, DID two-way, combination, inbound/outbound and both-way, and Directory Listing service. The PRI service shall interface to a VA-owned Voice over Internet Protocol (VoIP) telephone system to deliver the required telephone service. The Contractor shall install the PRI circuits with 1,000 new DID numbers. The existing Centrex service will remain in service 60 days after the new service is installed, at which time the VA will request the Centrex service and associated telephone equipment to be removed from the site. The Contractor shall port up to 100 existing telephone numbers from the Centrex service to the PRI service on the thirtieth (30^{th}) day after installation of the new PRIs. The Contractor shall ensure no interruption in service during the transition from existing Centrex service to new PRI service.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance shall be from date of award through September 30, 2015, with three 12-month options.

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 be performed in VA facilities located in HITC, First Avenue North of 22nd Street, Building 215, Hines, IL 60141.

4.3 TRAVEL

The Government does not anticipate travel under this effort to perform the tasks associated with the effort.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.1 PROJECT MANAGEMENT

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

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

Deliverables:

A. Contractor Project Management Plan

5.1.2 REPORTING REQUIREMENTS

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

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

The Report shall, at a minimum, contain the following information:

- Identify interruptions of service and/or outages encountered
    - How were problems resolved
    - If not resolved, what is plan of action to resolve including timeframes
- Any deviations from performance outlined in the CPMP
- On Demand Customer Service Record
- Number of response calls
    - Timeliness

  - Location
  - Problems encountered in restoring units to operational readiness
- Timeliness of Response Calls

In the first monthly report, the Contractor shall provide pertinent information gathered at the Kick Off Meeting.

The Contractor shall provide detailed information in the monthly progress report on Help Desk activity for the prior month. Activity information shall include number of tickets initiated; number of tickets closed; resolution for each ticket; date and time stamp information for each ticket, and the estimated date and resolution for closure on tickets remaining open that are carrying over to the next month.

The Contractor shall host monthly conference calls with the COR to keep him/her updated on the current status of services being provided, to discuss pending issues including actions being taken to resolve problems, and to make recommendations for contractual actions as appropriate. The Contractor shall document these calls in a Monthly Progress Report to the COR.

Deliverables:

A. Monthly Progress Report
B. Monthly Conference Call

5.1.2.1 ITEMIZED INVOICE

The Contractor shall provide the COR with a monthly itemized invoice to include the individual charges in a line-by-line item format with a detailed description of each charge in plain language that is easy to understand by a non-technical person. All billing codes used shall reference a legend to explain the billing code meaning. The Itemized invoice shall be provided in electronic form in Microsoft Excel. The Itemized invoice shall reflect the charges as of the last day of the preceding Month.

Deliverables:

A. Monthly Itemized Invoice

5.1.2.2 CUSTOMER SERVICE RECORDS (CSR)

The Contractor shall provide a Customer Service Record (CSR) to include all services and line information that is currently invoiced and provided under this Contract. The CSR shall contain detailed information about each separate line charge (i.e. type of service, federal access charge, number portability charge, calling blocks on the line, 911 charge, etc.) that encompasses the monthly service charge on the invoice. The CSR

shall provide the service location of the account, the billing address, directory listing information, hunting order, features that are being charged and on which line these features appear, calling plans that may include monthly charges, and taxes applied to each of the items on the record.

Deliverables:

A. Customer Service Record (CSR)

5.2 KICK OFF MEETING

The Contractor shall schedule the Kick-Off Meeting to be held within ten business days after contract award or as agreed upon between the VA Program Manager (PM)/COR and Contractor. The Contractor shall provide the agenda for the Kickoff meeting. The Kick-Off Meeting shall address post award topics and shall present the Contractor's plan and approach for meeting requirements. This shall include review of the CPMP and any detailed comments from the COR/PM on the CPMP shall be incorporated in the operational CPMP. The Kick-Off Meeting can be a virtual meeting.

Deliverables:

A. Kick Off Meeting

5.3 SERVICE TRANSITION

The Contractor shall develop a transition plan that includes milestones to transition the current Centrex service to the replacement ISDN PRI services. The draft Phase-In of Service Transition Plan shall outline the strategy and shall describe, in detail, the schedule and planned steps/milestones in assuming the operational responsibilities from the current Contractor. The Contractor shall provide the draft transition plan to the VA COR. The Contractor shall return a revised plan within 10 business days of receiving comments from VA. The Contractor shall not start the transition and circuit cutover until the COR and Enterprise Connectivity Chief approves the transition plan.

The installation of the new telephone service with a new block of 1,000 DID numbers shall occur within 60 days after contract award. The VA will connect the new telephone service to the VA-owned VoIP telephone system for testing purposes. The new service and existing service shall run concurrently up to 60 days to fully test the DID numbers and required line features with the VoIP telephone system. 100 existing telephone numbers shall be ported from the Centrex service to the new service on the 30th day after the installation of the PRI service with the approval of the COR. The Contractor shall submit a Letter of Authorization (LOA) including the telephone numbers to be transitioned to the new service. After the 60 day time period, the VA will arrange with the prior Contractor for disconnection of the Centrex service and removal of termination equipment and telephones from the property.

Deliverable:

A. Transition “Phase In” Plan

5.4 PRITRUNK LINES – HITC

The Contractor shall provide five ISDN lines at the PRI level of service consisting of 23 “B” voice channels and one (1) “D” signaling channel for each PRI using Facility Associated Signaling (FAS) on a redundant network. The Contractor shall provide PRI clocking on the circuits that shall interface with the existing VA owned VoIP telephone system. The total number of DID trunks shall be 115 for inbound/outbound and both-way service with outbound caller ID in one trunk group. The Presubscribed Interexchange Carrier (PIC) for Intra-LATA (Local Access and Transport Area) and Long Distance Calling shall be 0432, CenturyLink. The Contractor shall provide services to HITC First Avenue North of 22nd Street, Building 215, Hines, IL 60141. Calling name display information to be provided to called party shall be “Hines Data Center”.

5.5 DIRECT INWARD DIALING (DID)

The Contractor shall provide DID Service for five ISDN PRIs set up with 1 trunk group for inbound calling.

5.5.1 DID NUMBER BLOCK

The Contractor shall provide 1,000 numbers in blocks of 100 consecutive numbers with NPA (Numbering Plan Area Code) 708, 773 or 312. The Contractor shall provide the same NPA for all 1,000 numbers. The central office (exchange code) for the numbers shall end with 3, 4, 5, 6 or 7. The last four digits of the subscriber number shall start with 3, 4, 5, 6 or 7.

5.6 PORT EXISTING DIRECT INWARD DIALING (DID) NUMBERS

After award, the Contractor shall port up to 100 existing DID Telephone Numbers from the Centrex service to the new PRI service after installation. The Contractor shall submit a Letter of Authorization (LOA) to the incumbent carrier including the telephone numbers to be transitioned. The Contractor shall transition the telephone numbers after CO or COR approval and signature of the LOA. The service address for the existing DID Telephone Numbers to be ported is HITC, First Avenue North of 22nd Street, Building 215, Hines, IL 60141.

Deliverable:

A. Letter of Authorization

5.7 DIRECTORY LISTING/411 SERVICE

The Contractor shall provide Directory Listing/411 Service for one telephone number (708) 681-6601 located at First Avenue North of 22nd Street, Building 215, Hines, IL 60141.

All other telephone numbers associated with this request shall not be listed for Directory/411 Service.

5.8 TELECOMMUNICATION AVAILABILITY (UPTIME)

An availability of 99.995 percent shall be maintained for telecommunication services 24 hours per day, 7 days per week, 365 days per year.

Availability (uptime) percentage = (productive time –unscheduled downtime) / productive time x 100

Productive time is 24 hours per day, 7 days per week.

Unscheduled downtime begins at time of first service call until service is returned to proper operating conditions.

5.9 TELECOMMUNICATIONS SERVICE PRIORITY (TSP)

The TSP Program was developed to ensure priority treatment for the Nation's most important telecommunication services, services supporting National Security/Emergency Preparedness (NS/EP) missions. Following natural or technical disasters, telecommunications service vendors may become overwhelmed with requests for new services and requirements to restore existing services. The TSP Program authorizes and requires service vendors to provision and restore TSP-assigned services before non-TSP services. The TSP Program has two components: restoration and provisioning. A restoration priority is applied to new or existing telecommunication services to ensure their restoration before any non-TSP services. Priority restoration is necessary for a TSP service because interruptions may have a serious adverse effect on the supported NS/EP function.

All NS/EP missions fall into one of five TSP Program categories. All NS/EP telecommunication services qualify for some level of TSP protection. The level is determined in part by the category that represents the organization's mission. The five

categories are: (A) National Security Leadership, (B) National Security Posture and US Population Attack Warning, (C) Public Health, Safety, and Maintenance of Law and Order, (D) Public Welfare and Maintenance of the National Economic Posture, and (E) Emergency (Provisioning Requests Only). Categories A through D are referred to as "essential services".

Telecommunications services are designated as essential where a disruption of "a few minutes to one day" could seriously affect the continued operations that support an NS/EP function. Essential services are assigned a priority on a scale of 1 to 5 (with 1 as the highest priority) based on the appropriate subcategory. Services in subcategory A qualify for priority levels 1-5; those in subcategory B qualify for priority levels 2-5; those in subcategory C qualify for priority levels 3-5; and services in subcategory D qualify for priority levels 4-5.

The Contractor shall provide Telecommunications Service Priority Level 4 for these vital voice circuits which are considered critical for VA's nationwide operations.

5.9.2 INITIAL SETUP OF TSP

The Contractor shall facilitate and provide proof of certification of the initial setup of TSP for all circuits required in this PWS.

Deliverable:

A. TSP Setup Certification

5.9.3 RECURRING TSP DESIGNATION CERTIFICATION VALIDATION

The Contractor shall maintain the TSP designation certification is active for all circuits required in this PWS. The Contractor shall provide a report of the TSP Designation Certification Validation every 6 months.

Deliverable:

A. TSP Designation Certification Validation

5.10 HELP DESK

The Contractor shall provide a toll free number for customer service and Help Desk staffed by a live person 24 hours per day, 7 days per week, 365 days per year. The customer service support staff must be able to speak and write in English. The customer service support must not deploy the use of an Interactive Voice Response System (IVR). The Contractor shall provide a unique ticket number for each issue or request opened via email or telephone for tracking purposes and shall provide access to a web-based ticketing system that is updated on a daily basis with current status of the ticket.

The Contractor shall respond to all calls within two hours of call receipt. All high priority calls resolved and tickets closed within six hours of call. All medium priority calls resolved and tickets closed within eight hours. All low priority calls resolved and tickets closed within 24 hours. The Contractor shall enter all calls into a tracking database and log all problems to include date, time, priority, system, hardware or software, actions taken resolution/escalation.

The Contractor shall respond to email requests sent after hours on the next business day, unless an emergency has been declared.

The Contractor shall provide a single point of contact for any disputes.

5.11 APPLICABLE LINE FEES AND SURCHARGES

The Contractor shall itemize all line fees and surcharges. The total of all fees and surcharges shall not exceed 20% of the base line charges. These fees may include, but not limited to: port charges, line fees, federal universal service fees and access fees, as required by applicable law

5.12 OPTION PERIODS

If required, the Contractor shall complete the following tasks in Option Periods 1, 2 and 3.
Tasks: 5.1.2, 5.1.2.1, 5.1.2.2, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9.3, 5.10, 5.11

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.

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directive issued by the Office of Management and Budget (OMB) on September 28, 2010 (https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf) & (http://www.cybertelecom.org/dns/ipv6usg.htm). IPv6 technology, in accordance with the USGv6: A Technical Infrastructure for USGv6 Adoption (http://www.nist.gov/itl/antd/usgv6.cfm) and the NIST SP 800 series applicable compliance (http://csrc.nist.gov/publications/PubsSPs.html), shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 users, including all internal infrastructure and applications shall communicate using native IPv6 operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services, in addition to OMB/VA memoranda, can be found at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282.

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

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

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

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

used to build schedules to meet project requirements, regardless of the development methodology employed.

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

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

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

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

	Position Sensitivity and Background Investigation Requirements		
Task Number	Tier1 / Low/NACI	Tier 2 / Moderate/MBI	Tier 4 / High/BI
5.1	☒	☐	☐
5.2	☒	☐	☐
5.3	☒	☐	☐
5.4	☒	☐	☐
5.5	☒	☐	☐
5.6	☒	☐	☐
5.7	☒	☐	☐
5.8	☒	☐	☐
5.9	☒	☐	☐
5.10	☒	☐	☐
5.11	☒	☐	☐
5.12	☒	☐	☐

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

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
b. The Contractor shall bear the expense of obtaining background investigations.
c. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the ProPath template. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification

completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.

d. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
e. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
    1) For a Tier 1/Low Risk designation:
        a) OF-306
        b) DVA Memorandum – Electronic Fingerprints
    2) For Tier 2/Moderate or Tier 4/High Risk designation:
        a) OF-306
        b) VA Form 0710
        c) DVA Memorandum – Electronic Fingerprints
f. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
g. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via eQIP).
h. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
i. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or "Closed, No Issues" (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The

investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).

j. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
k. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.
l. Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

Deliverable:

A. Contractor Staff Roster

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

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

6.4 PERFORMANCE METRICS

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

Performance Objective	Performance Standard	Acceptable Performance Levels
5.1.1. CPMP Comprehensive project plan.	Written documentation describing proposed Project Plan in clear, concise wording.	Satisfactory or higher

Performance Objective	Performance Standard	Acceptable Performance Levels
5.1.2 Reporting	Detailed monthly progress report documenting work completed, help desk activity and regular attendance to monthly conference call	Satisfactory or higher
5.1.2.1 Itemized Invoice	Monthly invoice with individual charges and detailed description is plain language	Satisfactory or higher
5.1.2.2 Customer Service Records (CSR)	Written documentation describing all services and line information currently invoiced and provided.	Satisfactory or higher
5.2 Kickoff Meeting	Scheduled Conference Call, prepared agenda, participants notified in advance, with call-in telephone number and instructions	Satisfactory or higher
5.3 Service Transition	No interruption of service during transition	Less than 3 dropped or non working numbers inbound/outbound in a 4 hour period.
5.4 PRI Trunk Lines - HITC	Provide five (5) Integrated Services Digital Network (ISDN) lines consisting of 23 “B” voice channels and 1 D signaling channel.	Operational 99.99% of time
5.5 Direct Inward Dialing (DID)	Provide Direct Inward Dialing (DID) Service for (5) ISDN PRIs with 1 trunk group	Operational 99.99% of time
5.5.1 DID Number Block	Provide one (1) block of 1,000 consecutive numbers with NPA (Numbering Plan Area Code) 708, 773 or 312	Satisfactory or higher

Performance Objective	Performance Standard	Acceptable Performance Levels
5.6 Port Existing DID Numbers	Successful porting of up to 100 existing DID numbers from the Centrex service to the PRI service	No more than 2% of DID numbers not working during porting. Issues corrected within 4 hours of notification
5.7 Directory Listing/411 Service	Provide Directory Listing/411 Service for Published telephone numbers.	Satisfactory or higher
5.8 Telecommunication Availability (Uptime)	Report details network operations procedures and tasks to maintain equipment.	Satisfactory or higher
5.9 Telecommunications service priority (TSP)	Provide hardware and software necessary to successfully maintain Telecommunications Service Priority	Satisfactory or higher
5.9.1 Initial setup of TSP	Provide certification.	Satisfactory or higher
5.9.2 Recurring TSP Designation	Maintain the TSP designation certification	Satisfactory or higher

Performance Objective	Performance Standard	Acceptable Performance Levels
5.10 Help Desk	Input all calls into a tracking database. All calls responded to within two hours of call receipt. All high priority calls resolved and tickets closed within six hours of call. All medium priority calls resolved and tickets closed within eight hours. All low priority calls resolved and tickets closed within 24 hours. Properly log all problems to include date, time, priority, system, hardware or software, actions taken resolution/escalation	Satisfactory or higher

The Government will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable manner. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion.

6.5 FACILITY/RESOURCE PROVISIONS

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

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

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

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED. 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 athttps://www.tms.va.gov.If you do not have a TMS profile, go to https://www.tms.va.gov and click on the "Create New User" link on the TMS to gain access.

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

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at http://www.ea.oit.va.gov/index.asp in force at the time of issuance of this contract, including the Program Management Plan

and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP). VA reserves the right to assess contract deliverables for EA compliance prior to acceptance**.**

A2.1. VA Internet and Intranet Standards:

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

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

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

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

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

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

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and

Information Technology (EIT). These standards are found in their entirety at: 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.