PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS
Office of Information & Technology
Enterprise Systems Engineering
Integrated Campus Support

DEMARC at Hines OIFO and Building 37

Date: January 11, 2012
TAC-13-06660
PWS Version Number: 1.3

Contents

1.0 BACKGROUND

The mission of Department of Veterans Affairs (VA), Office of Information & Technology (OIT), Service Delivery and Engineering, Enterprise Systems Engineering is to provide benefits and services to Veterans of the United States. In meeting these goals, OIT strives to provide high quality, effective, and efficient Information Technology (IT) services to those responsible for providing care to the Veterans at the point-of-care as well as throughout all the points of the Veterans' health care in an effective, timely and compassionate manner. VA depends on Information Management/Information Technology (IM/IT) systems to meet mission goals.

VA requires continued support for connectivity and maintenance for the AS-13 Demarcation point (DEMARC) at the Hines Office of Information Field Offices (OIFO) including all associated recurring charges. Support includes connections for all T1/DS3 and OC48 Synchronous Optical Networking (SONET) Ring for the Hines OIFO and Bldg. 37. Monthly recurring service on the OC-48 Ring circuits riding on the SONET ring is also required.

2.0 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement (PWS), 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, "Personal Identity Verification of Federal Employees and Contractors," March 2006
4. Software Engineering Institute, Software Acquisition Capability Maturity Modeling (SA CMM) Level 2 procedures and processes
5. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
6. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
7. Department of Veterans Affairs (VA) Directive 0710, "Personnel Suitability and Security Program," May 18, 2007
8. VA Directive 6102, "Internet/Intranet Services," July 15, 2008
9. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
10. OMB Circular A-130, "Management of Federal Information Resources," November 28, 2000
11. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
12. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008

13. 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
14. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
15. VA Directive 6500, “Information Security Program,” August 4, 2006
16. VA Handbook 6500, “Information Security Program,” September 18, 2007
17. VA Handbook 6500.1, “Electronic Media Sanitization,” March 22, 2010
18. VA Handbook 6500.2, “Management of Security and Privacy Incidents,” June 17, 2008.
19. VA Handbook 6500.3, “Certification and Accreditation of VA Information Systems,” November 24, 2008.
20. VA Handbook, 6500.5, Incorporating Security and Privacy in System Development Lifecycle.
21. VA Handbook 6500.6, “Contract Security,” March 12, 2010
22. Technical Reference Model (TRM) (reference at http://trm.oit.va.gov/TRMHomePage.asp, or https://www.voa.va.gov/)
23. National Institute Standards and Technology (NIST) Special Publications
24. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008
25. VA Directive 6300, Records and Information Management, February 26, 2009
26. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010

3.0 SCOPE OF WORK

The Contractor shall provide connectivity and maintenance for the DEMARC, T1/DS3, and OC48 SONET Ring fiber optic network, including the Metropolitan Area Network (MAN). The Contractor shall provide connectivity services, as well as, support and repair both the actual fiber infrastructure and all associated equipment required for connectivity. The Contractor shall be responsible for the configuration and installation of any replacement equipment performed under maintenance.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance shall be 12-months from June 1, 2013 through May 31, 2014. At the discretion of the Government, two additional twelve-month option periods may be exercised.

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

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

Under current definitions, four are set by date:

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

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

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

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

4.2 PLACE OF PERFORMANCE

Tasks under this PWS shall be performed in VA facilities located in Hines, IL, Department of Veterans Affairs, Hines OIFO, 5th Avenue & Roosevelt Road, Building 37, Hines, IL 60141. Work may be performed at remote locations with prior approval of the Contracting Officer's Representative (COR).

4.3 TRAVEL

The Government anticipates no travel under this effort.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall provide the following specific tasks and deliverables.

5.1 CONNECTIVITY:

The Contractor shall provide service connectivity for the DEMARC, T1/DS3, OC-48 SONET bi-directional optical ring, and local serving wire-center with broadband connectivity. Both customer sites and Contractor locations are required to facilitate DS-1/DS-3 drop-off capabilities. The Contractor shall provide 99% network availability.

The Contractor shall provide a Monthly Status Report documenting system uptime and any down time root-cause analysis with an explanation for preventing future outages based on similar circumstances.

Deliverable:

A. Monthly Status Report

5.2 MAINTENANCE REQUIREMENTS

The Contractor shall maintenance for the DEMARC, T1/DS3, and SONET Ring equipment, including all associated MAN equipment 24 hours a day, 7 days a week. All configuration, installation, and repairs shall be performed by personnel that are industry certified and trained on a fiber based SONET OC48 and DS3. All maintenance performed shall be coordinated with the Contracting Officer Representative (COR). The Contractor shall report all activities in the Monthly Maintenance Log. Specific maintenance requirements are identified below:

A. The Contractor shall provide a designated point of contacts (including telephone numbers) to accept notifications for emergency, routine maintenance, and follow in service. In addition, the Contractor shall provide a single 24hr/7day phone number for the service of all equipment and communications lines.
B. The Contractor shall provide a preventive maintenance schedule. Preventive maintenance shall be performed in accordance with both data and telecommunications manufacture's recommended practice and service intervals during non-busy times agreed to by the Contractor Officer Representative (COR) and Contractor.
C. The Contractor shall respond via email or phone call to the COR to non-emergency (e.g. move, add, or change of ports events that can be scheduled) trouble calls within two hours after the receipt of the call. The repair process shall continue until completed. Remote repairs shall be completed within four hours from time of non-emergency call placement. The Contractor shall provide onsite maintenance if the problem is not resolved remotely within six hours of call placement unless an adequate service arrangement is agreed to by the COR.
D. An emergency maintenance (e.g. lost of circuits) call shall be deemed appropriate when a failure involves direct impact on patient care (i.e., the inability to transmit diagnostic images, failure of MAN to provide access to patient data). Emergency maintenance calls shall be resolved within four hours after the call is placed. The Contractor shall guarantee a two-hour acknowledgment time to emergency maintenance calls 365-days a year.
E. Non-emergency maintenance shall not be performed during normal working hours that would impair the operation of the MAN infrastructure.
F. Downtime shall not exceed 1% per month (based on a 24-hour day). Downtime is defined as equipment failure that results in failure to provide voice, video, or

data over the network that directly effects the operation of VA-OITFO. Scheduled downtimes are exempted.

G. The Contractor shall maintain existing multiplexors at each SONET point of demarcation and maintain the fault tolerant of the existing SONET ring network. The Contractor shall be required to support all SONET communications parts, services, and installation.
H. The Contractor shall provide detailed support documentation of all installed equipment including functional diagrams, equipment inventory with software revisions, and serial numbers. The vendor shall update the detailed support document within 10-days of any activity that causes a change to the documentation.
I. The Contractor shall provide a detailed Installation/Implementation Plan detailing 24X7 support of communication lines.
J. The Contractor shall provide technical liaison for support, operation, or fault resolution of communications problems that may be encountered on the Networx non-SONET portion of the MAN. The Contractor shall report and monitor repair progress in addition to reporting to the VA COR the Networx service status.

Deliverables:

A. Preventive Maintenance Schedule
B. Monthly Maintenance Log
C. POC List
D. Detailed Support Documentation
E. Installation/implementation Plan

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OIT 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 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 (http://www.cio.gov/documents/IPv6memofinal.pdf). IPv6 technology, in accordance with the USGv6 Profile (NIST Special Publication (SP) 500-267, http://www.antd.nist.gov/usgv6/) and NIST SP 800 series applicable compliance, 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 and all internal infrastructure and applications shall operate using native IPv6. To ensure interoperability, IPv4 will coexist during the transition to IPv6 and it is expected that VA will continue running IPv4 until it is phased out by 2015. By 2015, all computing, application, and network resources must turn off IPv4 as a communication mechanism in VA, unless a waiver is obtained from the Office of the Principal Deputy Assistant Secretary for Information and Technology, Department of Veterans Affairs or the device/service runs in an enclave.

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. However, the migration from Windows XP to Windows 7 is not yet complete within all of VA. As a result, compatibility with and support on Windows XP, Internet Explorer 7 and Microsoft Office 2007 are also required until April 2014 when Microsoft's extended support for Windows XP ends. Applications delivered to the VA and intended to be deployed to Windows XP or 7 workstation 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 VA trusted 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 has been configured using the Federal Desktop Core Configuration (FDCC) and 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 OIT 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 OIT-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 Security Suitability Program," Appendix A)
Low	**National Agency Check with Written Inquiries (NACI)** A 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	**Moderate Background Investigation (MBI)** A 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	**Background Investigation (BI)** A 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 is:

	Position Sensitivity and Background Investigation Requirements		
Task Number	Low/NACI	Moderate/MBI	High/BI
5.1	☒	☐	☐
5.2	☒	☐	☐

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. The roster shall contain the Contractor's Full Name, Full Social Security Number, Date of Birth, Place of Birth, and individual background investigation level requirement (based upon Section 6.2 Tasks).
d. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
e. For a Low Risk designation the following forms are required to be completed: 1.OF-306 and 2. DVA Memorandum – Electronic Fingerprints. For Moderate or High Risk the following forms are required to be completed: 1. VA Form 0710 and 2. DVA Memorandum – Electronic Fingerprints. These should be submitted to the COR within 5 business days after award.
f. The Contractor personnel will receive an email notification from the Security and Investigation Center (SIC), through the Electronics Questionnaire for Investigations Processes (e-QIP) identifying the website link that includes detailed instructions regarding completion of the investigation documents (SF85, SF85P, or SF 86). The Contractor personnel shall submit all required information related to their background investigations utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP).
g. The Contractor is to certify and release the e-QIP document, print and sign the signature pages, and send them to the COR for electronic submission to the SIC. These should be submitted to the COR within 3 business days of receipt of the e-QIP notification email.
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 termination of the contract for default.

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
1. Technical Needs	Shows understanding of requirements Efficient and effective in meeting requirements Meets technical needs and mission requirements Offers quality services/products	Satisfactory or higher

1a. SONET/MAN	Maintain SONET/MAN Availability 24/7	Not to exceed 1% downtime per month*
1b. Network Availability	Maintain & Provide Network Availability 24/7	99% Availability, measured on a monthly basis*
1c. Response to Trouble Calls	Responses received within 2 hours for emergency and non-emergency calls. Remote repairs completed within 4 hours of non-emergency call	100% of the time
2. Project Milestones and Schedule	Quick response capability Products completed, reviewed, delivered in timely manner Notifies customer in advance of potential problems	Satisfactory or higher
3. Project Staffing	Currency of expertise Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
4. Value Added	Provided valuable service to Government Services/products delivered were of desired quality	Satisfactory or higher

*The Government shall receive consideration on the following months invoice equal to the amount of downtime greater than 1%.

The Government will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the task order 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, 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, refer to ADDENDUM A and ADDENDUM B.

6.6 GOVERNMENT FURNISHED PROPERTY

Not applicable

ADDENDUM A

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)

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 are 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.

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.access-board.gov/sec508/standards.htm. 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

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the EIT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

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.

ADDENDUM B

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

Not applicable

B3. VA INFORMATION CUSTODIAL LANGUAGE

Not applicable

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

Not applicable

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

Not applicable

B6. SECURITY INCIDENT INVESTIGATION

Not applicable

B7. LIQUIDATED DAMAGES FOR DATA BREACH

Not applicable

B8. SECURITY CONTROLS COMPLIANCE TESTING

Not applicable

B9. TRAINING

Not applicable

Notes to the Contracting Officer

(This section to be removed from PWS before solicitation)

TYPE OF CONTRACT(S)

(Choose the type of contract that applies by selecting the checkbox, or, if a hybrid, select all that apply)

- ☒ Firm Fixed Price
- ☐ Cost Reimbursement
- ☐ Labor-Hour
- ☐ Time-and-Materials
- ☐ Other _____

SCHEDULE FOR DELIVERABLES

Note: Days used in the table below refer to calendar days unless otherwise stated. Deliverables with due dates falling on a weekend or holiday shall be submitted the following Government work day after the weekend or holiday.

Note: A ship to address must be provided for all hardware deliverables. Electronic submission of S/W or paper deliverables should be the norm unless otherwise stated. Email address(es) must be provided. Although email addresses are provided below for all POC's, table must be clear as to who receives the deliverables.

Task	Deliverable ID	Deliverable Description
5.1	A	**Monthly Status Report** Due 30 days after contract (DAC) and updated monthly thereafter. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
Error! Reference source not found.	A	**Preventive Maintenance Schedule** Draft due 10 DAC, final due 10 days after receipt of Government comments. Electronic submission to: VA PM, COR, CO Inspection: destination Acceptance: destination
	B	**Monthly Maintenance Log** Due 30 days after contract (DAC) and updated monthly thereafter. Electronic submission to: VA PM, COR, CO. Inspection: destination

		Acceptance: destination
	C	**POC List** Due 10 DAC Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
	D	**Detailed Support Documentation** Due 10 DAC and updated when equipment are maintained or upgraded. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
	E	**Installation/Implementation Plan** Due 30 DAC Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

(Note: If a deliverable is requested in draft, and then final submission-the deliverable line item is complete, no further update can be requested. Continued reporting should be a separate line item.)

INSPECTION and ACCEPTANCE / Free on board (FOB) for Shipped Deliverables

(NOTE: (Deliverables table reflects the Inspection and Acceptance) Include additional information if other than standard inspection and acceptance is required. If any hardware/software is being purchased (incidental to the service being performed), state the acceptance criteria and provide Shipping Address /Mark For requirements.

Inspection and acceptance shall be at ***<origin OR destination>*** and FOB shall be ***<origin OR destination OR indicate N/A > (N/A if the deliverable is a service item)*** Ship to address is: ***<enter all Address/Mark For requirements>***.

Special Shipping Instructions:

Prior to shipping, Contractor shall notify Site POCs, by phone followed by email, of all incoming deliveries including line-by-line details for review of requirements. Contractor shall not make any changes to the delivery schedule at the request of Site POC.

Contractors shall coordinate deliveries with Site POCs before shipment of <hardware> hardware to ensure sites have adequate storage space. All shipments, either single or multiple container deliveries, will bear the VA Purchase Order number on external shipping labels and associated manifests or packing lists. In the case of multiple container deliveries, a statement readable near the VA PO number shall indicate total number of containers for the complete shipment (i.e. “Package 1 of 2”), clearly readable on manifests and external shipping labels.

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

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

Total number of Containers: Package ___ of ___. (i.e., Package 1 of 3)

NOTE: VA XXX Initiative ***(if applicable)***

POINTS OF CONTACT

VA Program Manager:
Name: Joe Gibbons
Address: Department of Veterans Affairs, 113 Holland Avenue, Albany, NY 12208
Voice: 518-449-0618
Email: Joe.Gibbons@va.gov

Contracting Officer’s Representative:
Name: Joe Gibbons
Address: Department of Veterans Affairs, 113 Holland Avenue, Albany, NY 12208
Voice: 518-449-0618
Email: Joe.Gibbons@va.gov

Contracting Officer:
Name:
Address:
Voice:
Email:

ADDITIONAL ITEMS

GOVERNMENT RESPONSIBILITIES

The following needs to be provided by the CO to the Contractor:

1. The Security Investigations Center will require the following forms from the Contractor or to the Contractor's personnel:
    a. 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. The roster shall contain the Contractor's Full Name, Full Social Security Number, Date of Birth, Place of Birth, and individual background investigation level requirement (based upon Section 6.2 Tasks).
    b. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
    c. For a Low Risk designation the following forms are required to be completed: 1.OF-306 and 2. DVA Memorandum – Electronic Fingerprints. For Moderate or High Risk the following forms are required to be completed: 1. VA Form 0710 and 2. DVA Memorandum – Electronic Fingerprints. These should be submitted to the COR within 5 business days after award. (DVA Memorandum – Electronic Fingerprints is filled out by the VA Facility that took the electronic fingerprints)
    d. The Contractor personnel will receive an email notification from the Security and Investigation Center (SIC), through the Electronics Questionnaire for Investigations Processes (e-QIP) identifying the website link that includes detailed instructions regarding completion of the investigation documents (SF85, SF85P, or SF 86). (The SF85 does not need to be uploaded because OPM is going paperless and the contractor will complete this questionnaire online when the e-QIP link is sent.) (DVA Memorandum – Electronic Fingerprints is filled out by the VA Facility that took the electronic fingerprints) (Please be advised that the contractor will need all the necessary information easily accessible as the website will time out and they can lose the information they inputted if they take too long to fill it in.)The Contractor personnel shall submit all required information related to their background investigations utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP).
    e. The Contractor is to certify and release the e-QIP document, print and sign the signature pages, and send them to the COR for electronic submission to the SIC. These should be submitted to the COR within 3 business days of receipt of the e-QIP notification email.
    f. The SIC will then upload the e-QIP signature pages to e-QIP and release the case file to OPM for investigation.

g. The SIC will notify the CO and Contractor after adjudicating the results of the background investigations received from OMB.

SPECIAL INSTRUCTIONS/REMARKS

(Include delivery instructions; required Delivery dates in terms of number of days after receipt of order (ARO) or days after contract (DAC); where is equipment going; mark for requirements (name of a person)/receiving contact; prior year PO#s, proposed payment provisions; Government furnished property; suggested contract clauses; other valuable information, etc., as applicable). Provide additional documentation if needed.

SPECIAL CLAUSES, ETC. TO BE INCLUDED IN THE SOLICITATION

(Choose Special Clause(s), etc., if applicable, by selecting the checkbox and modifying as necessary)

☐ Transition clause required?
(Insert FAR clause, Continuity of Services, FAR 52.237-3)
☐ Intellectual Property/Technical Data Rights Clause required?
☐ OCI Clause required?
☐ Government Furnished Material/Equipment: CO should add a special clause to the contract citing the Title of the material/equipment, Identifier (Serial Number), Quantity, Purpose, and Date required by Contractor.
☐ Other _____
☐ Other _____

FOR TAC USE ONLY---SECURITY RELATED GUIDANCE

☒ **(Always Checked for Services)** Addendum B Security Requirement guidance to CO within Addendum B, Section B9 Training, Para. a) Sub Para. d,

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.]***

SECURITY CHECKLIST REQUIREMENTS-- ***(If the customer answers yes to questions 4, 5, 6, and/or 7 on the Information Security Checklist, then follow the steps indicated. With the exception of question #7, if the customer answers No to any of the questions, then no action is required for those questions)***

☐ Yes ☒ No Question 4: Contracting Officials need to work with the Program Manager or (procurement requestor), COR, PO, and ISO to (IF YES):

i. Include the appropriate risk designation of the Contractors based on the PDAT determination. ***(Contractor Personnel Security Requirements are covered in Section 6.2 of this PWS)***
ii. Incorporate the security clause (Appendix B) into the contract involved and the appropriate security/privacy language outlined in Appendix C into the solicitation. ***(Include Addendum B in PWS)***
iii. Determine if protected health information is disclosed or accessed and if a BAA is required.***(CO to Provide BAA Assistance (Using Nov 2008 version of BAA (approved by OGC) and coordinate with BAA Manager)***

☐ Yes ☒ No Question 5: Incorporate the clause from Appendix B and the appropriate security/privacy language from Appendix C respectively into the solicitation and contract and initiate planning for the certification and accreditation of the Contractor system(s). Contracting Officials need to work with the COR and ISO to (IF YES):

- Determine the security impact of the IT system as High, Moderate, or Low per 6500 Handbook, *Information Security Program****. (Covered in Contractor Personnel Security Requirements Section 6.2)***
- Ensure Contractor understanding of the IT security requirements for certification and accreditation (authorization) (C&A) of the Contractor system. See VA Handbook 6500.3, *Certification and Accreditation*. ***(CO to notify COR of this responsibility in letter to COR)***
- Ensure that the proper VA Management Official is appointed by the Certification Program Office to formally authorize operation of the system in accordance with VA Handbook 6500 and 6500.3. ***(CO to notify COR of this responsibility in letter to COR)***
- Enforce Contractor performance (timely submission of deliverables, compliance with personnel screening requirements, maintenance of secure system configurations and participation in annual IT Federal Information Security Management Act (FISMA) assessments to ensure compliance with FISMA requirements). ***(CO to notify COR of this responsibility in letter to COR)***
- Ensure yearly FISMA assessments are completed and uploaded into SMART. ***(CO to notify COR of this responsibility in letter to COR)***

☐ Yes ☒ No Question 6: Incorporate the security clause from Appendix B and the appropriate security/privacy language from Appendix C respectively into the solicitation and contract. Contracting Officials need to work with the COR and the ISO to (IF YES):

- Ensure Contractor understands and implements the IT security requirements for system interconnection documents required per the Memorandum of Understanding or Interconnection Agreement (MOU-ISA). The standard operating procedure (SOP) and a template for a MOU-ISA are located on the Information Protection Risk Management (IPRM) Portal and can be provided to the Contractor. (***CO to notify COR of this responsibility in letter to COR and supply MOU-ISA template)***
- Ensure Contractor understands their participation in IT security requirements for C&A of the VA system to which they connect ***(CO to notify COR of this responsibility in letter to COR)***
- Enforce Contractor performance (timely submission of deliverables, compliance with personnel screening requirements, and appropriate termination activity as appropriate). ***(CO to notify COR of this responsibility in letter to COR)***

IF NO:

- Include a statement in PWS, immediately following the Security Clause Section that *"The C&A Requirements do not apply and that a Security Accreditation Package is not required".*

☐ Yes ☒ No Question 7: Incorporate the security clause and the appropriate security language from Appendices B and C into the solicitation and contract. The COR needs to (IF YES):

- Ensure that a Contractor Security Control Assessment (CSCA) is completed within 30 days of contract approval and yearly on the renewal date of the contract. ***(CO to notify COR of this responsibility in letter to COR and to supply CSCA Document-Self Assessment Questionnaire for Contract Service Providers)***
- Ensure that the CSCA is sent to the ISO and the OCS Certification Program Office for review to ensure that appropriate security controls are being implemented in service contracts. ***(CO to notify COR of this responsibility in letter to COR)***
- Ensure a copy of the CSCA is maintained in the Security Management and Reporting Tool (SMART) database. COR will provide a copy of the completed CSCA to ISO for uploading into SMART database***. (CO to notify COR of this responsibility in letter to COR)***

☒ **(Always Checked for Services)** Contractor Rules of Behavior-Appendix D in Handbook 6500.6 – (CO to add to solicitation, CO to ensure Contractor signs document)

ADDITIONAL NOTES TO PREPARER

1. ***Run Spell Check and Grammar Check in document for final review. Simple and easy tool to utilize and benefit from.***
2. ***When listing/itemizing points, keep the outline consistent (use appropriate number or letter, versus a bullet).***
3. ***If deliverables need to be submitted in draft form, timeframes must be stated. Reference example provided in the table above.***
4. ***Other submissions may be required but not held to draft/comment/final submissions. For example, monthly status reports are due 5 days after the conclusion of the reporting period (end of month).***
5. ***Customer must identify which deliverables continue if option years are exercised. Not all deliverables would necessarily repeat. Certain deliverables are final in the base year.***
6. ***Do not put due dates in "Deliverables:" section of task, rather include timeframes/due dates in "Schedule for Deliverables" table above. Also ensure customer deliverables are detailed in the narrative of the task to include format and content requirements.***
7. ***Ensure deliverables in tasks match deliverables in table.***
8. ***If PMAS applies, ensure deliverables are delivered in 6 month increments.***
9. ***Deliverable due dates should be in terms of number of days after award or based on an event.***
10. ***If for some reason the deliverable must be submitted in hard copy or on CD, be sure to specify the requirement within the line item. Also, in this case identify number of copies and mailing address.***
11. ***Each deliverable line item must cite inspection and acceptance criteria; Inspection: Origin or Destination; Acceptance: Origin or Destination (most likely destination on both).***
12. ***Update the Table of Contents by hitting F9.***