SIMPLIFIED ACQUISITION PROCEDURES (SAP) PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS

Department of Veterans Affairs, VHA, Office of Veterans Access to Care.
Manila Kiosk Deployment Support

Date: *March 1, 2017*
PWS Version Number: *1.0*

Contents

1.0 DESCRIPTION OF SERVICES

The Contractor shall provide support to the VA for the installation and operation of kiosks at the Manila VA Hospital. This support shall include remote site and onsite verification of kiosks locations; pre-deployment activities and deployment activities for the kiosks; and grand opening week support.

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. 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. VA Directive 0710, “Personnel Suitability and Security Program,” June 4, 2010, http://www1.va.gov/vapubs/
8. VA Handbook 0710, Personnel Suitability and Security Program”, May 2, 2016, http://www1.va.gov/vapubs/
9. VA Directive and Handbook 6102, “Internet/Intranet Services,” July 15, 2008
10. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
11. OMB Circular A-130, “Managing Federal Information as a Strategic Resource,” July 28, 2016
12. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
13. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
14. 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
15. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
16. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, 2012
17. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” March 10, 2015
18. VA Handbook 6500.1, “Electronic Media Sanitization,” November 03, 2008
19. VA Handbook 6500.2, “Management of Breaches Involving Sensitive Personal Information (SPI)”, July 28, 2016

20. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring Of VA Information Systems,” February 3, 2014
21. VA Handbook, 6500.5, “Incorporating Security and Privacy in System Development Lifecycle”, March 22, 2010
22. VA Handbook 6500.6, “Contract Security,” March 12, 2010
23. VA Handbook 6500.8, “Information System Contingency Planning”, April 6, 2011
24. OI&T ProPath Process Methodology (Transitioning to Process Asset Library (PAL) (reference process maps at http://www.va.gov/PROPATH/Maps.asp and templates at http://www.va.gov/PROPATH/Templates.asp
25. One VA Technical Reference Model (TRM) (reference at http://www.va.gov/trm/TRMHomePage.aspx)
26. National Institute Standards and Technology (NIST) Special Publications
27. VA Directive 6508, Implementation of Privacy Threshold Analysis and VA Privacy Impact Assessment, October 15, 2014
28. VA Handbook 6508.1, “Procedures for Privacy Threshold Analysis and Privacy Impact Assessment,” July 30, 2015
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, October 26, 2015
33. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 24, 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 SP 800-157, Guidelines for Derived PIV Credentials, December 2014
43. NIST SP 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 https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
47. IAM Identity Management Business Requirements Guidance document, May 2013, (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, Department of Homeland Security, October 1, 2013, https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf
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 13693, "Planning for Federal Sustainability in the Next Decade", dated March 19, 2015
55. Executive Order 13221, "Energy-Efficient Standby Power Devices," August 2, 2001
56. VA Directive 0058, "VA Green Purchasing Program", July 19, 2013
57. VA Handbook 0058, "VA Green Purchasing Program", July 19, 2013
58. Office of Information Security (OIS) VAIQ #7424808 Memorandum, "Remote Access", January 15, 2014, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
59. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
60. VA Memorandum, "Implementation of Federal Personal Identity Verification (PIV) Credentials for Federal and Contractor Access to VA IT Systems",

(VAIQ# 7614373) July 9, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28

61. VA Memorandum "Mandatory Use of PIV Multifactor Authentication to VA Information System" (VAIQ# 7613595), June 30, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
62. VA Memorandum "Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges" (VAIQ# 7613597), June 30, 2015; https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
63. "Veteran Focused Integration Process (VIP) Guide 1.0", December, 2015, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371
64. "VIP Release Process Guide", Version 1.4, May 2016, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4411
65. "POLARIS User Guide", Version 1.2, February 2016, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4412

3.0 PERFORMANCE DETAILS

3.1 PERFORMANCE PERIOD

The period of performance (PoP) shall be from the date of award through 30 days.

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

3.2 PLACE OF PERFORMANCE

Tasks under this PWS shall be performed in VA facilities located in Manila VA Hospital, Manila Philippines.

4.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

The remote site verification support shall include coordinating with Manila OIT staff to verify ACL/VLAN settings and that they have been applied. The Contractor shall also verify network connectivity, ACL settings, URL access from clerk computers, connectivity speed, and performance.

During deployment, the Contractor shall at a minimum:
1) Performance of Site Assessment/Pre-Implementation Site Readiness Support: Coordinate with local logistics for delivery times and receipt of hardware
2) Coordinate with local logistics and VPS Asset Manager for correct EIL, IP, and MAC Addresses
3) Load and unload kiosks and inspect for damages

4) Stage kiosks in the appropriate facility locations
5) Site Implementation kiosk/Configuration & Implementation of Server(s).
6) Install kiosks and ensure each kiosk works and the entire VetLink network works within Manila VA Facility.

The grand opening week support shall include the following:

- Provide onsite staff to support Veteran usage of kiosks and assist clinic staff with the application and deskside coaching
- Adjust application configurations based on site requests and clinic workflows
- Document issues and best practices report for the Week Summary Report
- Verify application reports and report data
- Document site's final workflow configuration workbook

The Contractor shall also provide a project plan, schedule, and staff roster within five days of award.

4.1 REPORTING REQUIREMENTS

The Contractor shall provide the COR with Weekly Progress Reports in electronic form in Microsoft Word and Project formats. The report shall include detailed instructions/explanations for each required data element, to ensure that data is accurate and consistent.

The Weekly 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 report shall also include an itemized list of all Electronic and Information Technology (EIT) deliverables and their current Section 508 conformance status. 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.

Deliverable:

A. Weekly Progress Report

4.2 PROJECT MANAGEMENT PLAN

Contractor shall provide a Project Management Plan that details all work requirements described above. The plan shall be delivered 5 days after award to the COR.

Deliverable:

A. Project Management Plan

4.3 ENTERPRISE AND IT FRAMEWORK

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

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are PIV-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), http://www.ea.oit.va.gov/VA_EA/VAEA_TechnicalArchitecture.asp, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/enterprise_dp.asp. The Contractor shall ensure all Contractor delivered applications and systems are compliant with VA Identity Management Policy (VAIQ# 7011145), Continued Implementation of Homeland Security Presidential Directive 12 (VAIQ#7100147), and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document), located at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514. The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63, VA Handbook 6500 Appendix F, “VA System Security Controls”, and VA IAM enterprise requirements for direct, assertion based authentication, and/or trust based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of Personal Identity Verification (PIV) and/or Common Access Card (CAC), as determined by the business need. Assertion based authentication must include a SAML implementation. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST 800-63 guidelines. Trust based authentication must include authentication/account binding based on trusted HTTP headers. The Contractor solution shall conform to the specific Identity and Access Management PIV requirements set forth in OMB Memoranda M-04-04, M-05-24, M-11-11, as well as the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, and supporting NIST Special Publications. OMB Memoranda M-04-04, M-05-24, and M-11-11 can be found at: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-04.pdf,

https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-24.pdf, and https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf respectively. The identity authentication Level of Assurance (LOA) requirement for this specific effort is LOA-4.

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directives issued by the Office of Management and Budget (OMB) on August 2, 2005 (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf) and September 28, 2010 (https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf). IPv6 technology, in accordance with the USGv6 Profile (NIST Special Publication (SP) 500-267 (http://www-x.antd.nist.gov/usgv6/index.html), the 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. In addition to the above requirements, all devices shall support native IPv6 and/or dual stack IPv6 IPv4 connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 and/or dual stack IPv6 IPv4 users and all internal infrastructure and applications shall communicate using native IPv6 and/or dual stack IPv6 IPv4 operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services in dual stack solutions, in addition to OMB/VA memoranda, can be found at: https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282.

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf), M08-23 mandating Domain Name System Security (NSSEC) (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf.

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 11 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Office 2013 and Windows 8.1. However, Office 2013 and Windows 8.1 are not the VA standard yet and are currently not approved for use on the VA Network, but are in-process for future approval by OI&T. Upon the release approval of Office 2013 and Windows 8.1 individually as the VA standard, Office 2013 and

Windows 8.1 will supersede Office 2010 and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be delivered as a signed .msi package and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA's current desktop application deployment tool. Signing of the software code shall be through a vendor provided certificate that is trusted by the VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) specific to the particular client operating system being used.

The Contractor shall support VA efforts IAW the Veteran Focused Integration Process (VIP). VIP is a Lean-Agile framework that services the interest of Veterans through the efficient streamlining of activities that occur within the enterprise. The VIP Guide can be found at https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371. The VIP framework creates an environment delivering more frequent releases through a deeper application of Agile practices. In parallel with a single integrated release process, VIP will increase cross-organizational and business stakeholder engagement, provide greater visibility into projects, increase Agile adoption and institute a predictive delivery cadence. VIP is now the single authoritative process that IT projects must follow to ensure development and delivery of IT products

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

4.4 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).

4.5 PERFORMANCE METRICS

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

Performance Objective	Performance Standard	Acceptable Levels of Performance

A. Technical / Quality of Product or Service	1. Demonstrates understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Provides quality services/products	Satisfactory or higher
B. Project Milestones and Schedule	1. Established milestones and project dates are met 2. Products completed, reviewed, delivered in accordance with the established schedule 3. Notifies customer in advance of potential problems	Satisfactory or higher

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

6. SECURITY – PRIVACY REQUIREMENTS

General - All contractors and contractor personnel shall be subject to the same Federal laws, regulations, standards and VA policies as VA, and VA personnel, regarding information and information system security. Contractors must follow policies and procedures outlined in VA Directive 6500, Information Security Program and its handbooks to ensure appropriate security controls are in place.

INFORMATION SYSTEM SECURITY
The contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard contract language, conditions laws, and regulations. The contractor's firewall and web server shall meet or exceed the government minimum requirements for security. All government data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA project manager and the VBA Headquarters 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 accreditation.

The contractor and their personnel shall be subject to the same Federal laws, regulations, standards and VA policies as VA personnel, regarding information and information system security. These include, but are not limited to Federal Information Security Management Act (FISMA), Appendix III of OMB Circular A-130, and guidance and standards, available from the Department of Commerce's National Institute of Standards and Technology (NIST). This also includes the use of common security configurations available from NIST's Web site at:
http://checklists.nist.gov

To ensure that appropriate security controls are in place, Contractors must follow the procedures set forth in "VA Information and Information System Security/Privacy Requirements for IT Contracts" located at the following Web site:
http://www.iprm.oit.va.gov."

Access to va information and va information systems

A contractor shall request logical (technical) and/or physical access to va information and va information systems for employees, subcontractors, and affiliates only to the extent necessary: (1) to perform the services specified in the contract, (2) to perform necessary maintenance functions for electronic storage or transmission media necessary for performance of the contract, and (3) for individuals who first satisfy the same conditions, requirements and restrictions that comparable va employees must meet in order to have access to the same type of va information.

All contractors and subcontractors working with va sensitive information are subject to the same investigative requirements as those of regular va appointees or employees who have access to the same types of information. The level of background security investigation will be in accordance with va directive 0710, handbook 0710, which are available at: http://www1.va.gov/vapubs/ and vha directive 0710 and implementing handbook 0710.01 which are available at.:
http://www1.va.gov/vhapublications/index.cfm contractors are responsible for screening their employees. The following are va's approved policy exceptions for meeting va's background screenings/investigative requirements for certain types of contractors:

Contract personnel not accessing va information resources such as personnel hired to maintain the medical facility grounds, construction contracts, utility system contractors, etc.,

Contract personnel with limited and intermittent access to equipment connected to facility networks on which no va sensitive information is available, including contractors who install, maintain, and repair networked building equipment such as fire alarm; heating, ventilation, and air conditioning equipment; elevator control systems, etc. If

equipment to be repaired is located within sensitive areas (e.g. Computer room/communications closets) va it staff must escort contractors while on site.

Contract personnel with limited and intermittent access to equipment connected to facility networks on which limited va sensitive information may reside, including medical equipment contractors who install, maintain, and repair networked medical equipment such as ct scanners, ekg systems, icu monitoring, etc. In this case, veterans health administration facilities must have a duly executed va business associate agreement (baa) in place with the vendor in accordance with vha handbook 1600.01, business associates, to assure compliance with the health insurance portability and accountability act of 1996 (hipaa) in addition to the contract. Contract personnel, if on site, should be escorted by va it staff.

Contract personnel who require access to national security programs must have a valid security clearance. National industrial security program (nisp) was established by executive order 12829 to ensure that cleared u.s. Defense industry safeguards the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. Defense security service (dss) administers the nisp on behalf of the department of defense and 23 other federal agencies within the executive branch. Va will verify clearance through dss.

Va information custodial requirements

Information made available to the contractor by va for the performance or administration of this contract or information developed by the contractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the contracting officer. This clause expressly limits the contractor's rights to use data as described in rights in data - general, far 52.227-14(d) (1).

Information generated by a contractor as a part of the contractor’s normal business operations, such as medical records created in the course of providing treatment, is subject to a review by the office of general counsel (ogc) to determine if the information is the property of va and subject to va policy. If the information is determined by ogc to not be the property of va, the restrictions required for va information will not apply.

Va information will not be co-mingled with any other data on the contractors and, or subcontractors information systems/media storage systems in order to ensure va requirements related to data protection and media sanitization can be met. Va also reserves the right to conduct it resource inspections to ensure data separation and on-site inspection of information destruction/media sanitization procedures to ensure they are in compliance with va policy requirements.

Prior to termination or completion of this contract, contractor will not destroy information received from va or gathered or created by the contractor in the course of performing

this contract without prior written approval by the va contracting officer. Any data destruction done on behalf of va by a contractor must be done in accordance with national archives and records administration (nara) requirements as outlined in va directive 6300, records and information management and its handbook 6300.1 records management procedures, and applicable va records control schedules.

The contractor will receive, gather, store, back up, maintain, use, disclose and dispose of va information only in compliance with the terms of the contract and applicable federal and va information confidentiality and security laws, regulations and policies. Applicable federal information security regulations include all federal information processing standards (fips) and special publications (sp) issued by the national institute of standards and technology (nist). If federal or va information confidentiality and security laws, regulations and policies become applicable to the va information or information systems after execution of the contract, or if nist issues or updates applicable fips after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies, including fips or sp, in this contract.

Contractors collecting, storing, or disseminating personal identifiable information (pii) or protected health information (phi) data must conform to all pertinent regulations, laws, and va directives related to privacy. Contractors must provide access for va privacy reviews and assessments and provide appropriate documentation as directed.

The contractor shall not make copies of va information except as necessary to perform the terms of the agreement or to preserve electronic information stored on contractor electronic storage media for restoration in case any electronic equipment or data used by the contractor needs to be restored to an operating state.

If va determines that the contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for va to terminate the contract for default or terminate for cause under federal acquisition regulation (“far”) part 12.

If a vha contract is terminated for cause, the associated business associate agreement (baa) will also be terminated and appropriate actions taken in accordance with vha handbook 1600.01 business associates.

Contractor will store, transport or transmit va sensitive information in an encrypted form, using a va-approved encryption application that meets the requirements of nist’s fips 140-2 standard.

The contractor’s firewall and web services security controls, if applicable, shall meet or exceed va’s minimum requirements. Va directives are available on the va directives web site at http://www1.va.gov/vapubs/.

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

Notwithstanding the provision above, the contractor shall not release medical quality assurance records protected by 38 u.s.c. 5705 or records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus protected under 38 u.s.c. 7332 under any circumstances, including in response to a court order, and shall immediately refer such court orders or other inquiries to the va contracting officer for response.

The contractor will not use technologies banned in va in meeting the requirements of the contract (e.g., bluetooth enabled devices).

information system design and development

Information systems that are designed or developed for or on behalf of va at non-va facilities shall comply with all va policies developed in accordance with federal information security management act (fisma), health insurance portability and accountability act (hipaa), nist, and related va security and privacy control requirements for federal information systems. This includes standards for the protection of electronic phi, outlined in 45 c.f.r. Part 164, subpart c, information and system security categorization level designations in accordance with fips 199 and fips 200 with implementation of all baseline security controls commensurate with the fips 199 system security categorization (reference appendix d of va handbook 6500, va information security program). During the development cycle a privacy impact assessment will be completed, provided to the cor, and approved by the va privacy service in accordance with va privacy impact assessment handbook 6500.3.

The security controls must be designed, developed, approved by va, and implemented in accordance with the provisions of va security system development life cycle as outlined in nist special publication 800-37 and va handbook 6500.

The contractor will be required to design, develop, or operate a system of records on individuals to accomplish an agency function subject to the privacy act of 1974, (as amended), public law 93-579, december 31, 1974 (5 u.s.c.552a) and applicable agency regulations. Violation of the privacy act may involve the imposition of criminal and civil penalties.

The contractor agrees to -

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

- the systems of records; and
- the design, development, or operation work that the contractor is to perform;

Include the privacy act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the act; and,

Include this privacy act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

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

Operation of a system of records" means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

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

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

Information system hosting, operation, maintenance or use

For information systems that are hosted, operated, maintained, or used on behalf of va at non-va facilities, contractors are fully responsible and accountable for ensuring compliance with all hipaa, privacy act, fisma, nist, fips, and va security and privacy

directives and handbooks. The contractor security control procedures must be identical, not equivalent, to those procedures used to secure va systems. A privacy impact assessment (pia) must also be provided to the cor and approved by va privacy service prior to operational approval. All external internet connections involving va information must be reviewed and approved by va prior to implementation.

Adequate security controls for collecting, processing, transmitting, and storing of personally identifiable information, as determined by the va privacy service, must be in place, tested, and approved by va prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of va. These security controls need to be stated within the pia and supported by a risk assessment. If these controls are determined not to be in place, or inadequate, a plan of action and milestones (poa&m) must be submitted and approved prior to the collection of pii.

Outsourcing (contractor facility/contractor equipment/contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (c&a) of the contractor's systems in accordance with nist special publication 800-37 and va handbook 6500 and a privacy impact assessment of the contractor's systems prior to operation of the systems. Government-owned (government facility/government equipment) contractor-operated systems, third party or business partner networks require a system interconnection agreement and a memorandum of understanding (mou) which detail what data types will be shared, who will have access, and the appropriate level of security controls for all systems connected to va networks.

Assessment and authorization (a&a)
The certification and accreditation (c&a) process is also known as assessment and authorization (a&a). Va handbook 6500.6 and va handbook 6500.3 provide guidance to contractors to develop and host information systems that contain va data. Nist and omb policies and procedures concerning information system a&a include but are not limited to continuous monitoring and quarterly vulnerability scanning. The current security accreditation status of the contractor's solution must be documented by the system security plan (ssp), authority to operate (ato) determination letter, or third-party security accreditation (i.e. Ssae-1 6, diacap). The contractor must have an approved computer system that will allow it to begin processing va data as soon as personnel are approved for work (having met training and background requirements). Va personnel will review provided documentation to ensure the contractor meets agency's policies and standards concerning information security before the system is authorized for use. Successfully meeting the a&a requirements will enable the system to be used in production.

The contractor shall develop and maintain a system a&a package. The contractor shall be responsible for security control testing by an independent third party test organization as defined by nist 800-37, rev. I in conjunction with the security controls in the moderate-impact baseline as defined nist sp 800-53, rev. 4.

The contractor shall provide all system documentation required for certification and work with va personnel to facilitate the successful completion of the a&a process.
The system a&a package shall consist of the following documents:

Table 5.4: system a&a package documents
1. System security plan (guidance is found in nist sp 800-18 and by using the va risk assessment review checklist and the government risk and compliance (grc) riskvision automated tool.)
2. Risk assessment (guidance is found in nist sp 800-30 and by using the va risk assessment review checklist and the government risk and compliance (grc) riskvision automated tool.)
3. Signatory authority
    a) guidance is found in nist sp 800-18.
    b) all package submissions must include this document signed and dated by the appropriate parties.
4. Contingency plan (guidance is found in nist sp 800-34 and va handbook 6500.)
5. Incident response plan (guidance is found in nist sp 800-61 and va handbook 6500.)
    a) nsoc is responsible for national level tasks associated with incident response. Each site is responsible for developing local level procedures incorporating nsoc areas or responsibility.

6. Configuration management plan (guidance is found in nist sp 800-70 and va handbook 6500.)
7. Security configuration checklists (guidance is found in nist sp 800-70.)
8. System interconnection agreements (guidance is found in nist sp 800-47 and va handbook 6500.)

The contractor must adhere to all fisma, fips, and nist standards related to the annual fisma security controls assessment and review and update the pia. Any deficiencies noted during this assessment must be provided to the va contracting officer and the information security officer (iso) for entry into va's plan of action and milestone (poa&m) management process. The contractor will use va's poa&m process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the government. Contractor procedures will be subject to periodic, unannounced assessments by va officials. The physical security aspects associated with contractor activities will also be subject to such assessments. As updates to the system occur, an updated pia must be submitted to the va privacy service through the cor for approval.

All electronic storage media used on non-va leased or owned it equipment that is used to store, process, or access va sensitive information must have all va sensitive information removed, cleared, sanitized, or destroyed in accordance with va policies and procedures upon: (1) completion or termination of the contract or (2) disposal or

return of the it equipment by the contractor or any person acting on behalf of the contractor, whichever is earlier.

Security incident investigation

For unauthorized access to, loss or damage to va assets, or sensitive information, or an action that breaches va security procedures, the contractor shall immediately notify the cor and simultaneously, the designated iso/privacy officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor has access.

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

The contractor will simultaneously report the incident to the appropriate law enforcement entity(ies) of jurisdiction, including the va offices of the inspector general and security and law enforcement, in instances of theft or break-in or other criminal activity. The contractor, its employees, and its subcontractors and their employees will cooperate with va and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The contractor will cooperate with va in any civil litigation to recover va information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

To the extent practicable, the contractor shall mitigate any harmful effects on individuals whose va information was accessed or disclosed in a security incident. In the event of a data breach with respect to any va sensitive information processed or maintained by the contractor or subcontractor under the contract, the contractor is responsible for liquidated damages to be paid to va.

Security controls compliance testing

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

Security training

All contractor employees and sub-contractor employees requiring access to va sensitive information and/or va information systems shall complete the following before being granted access to va networks or sensitive information:

- sign and acknowledge understanding of and responsibilities for compliance with the attached national rules of behavior relating to access to va information and information systems;
- successfully complete va cyber security awareness training and annual refresher training as required;

- successfully complete va general privacy training and annual refresher training as required; and

- 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.]

The contractor shall provide to the contracting officer a copy of the training certificates for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required. These online courses are located at the following web site: https://www.ees-learning.net/.

Failure to complete this mandatory training within the timeframe required will be grounds for suspension or termination of all physical and/or electronic access privileges and removal from work on the contract until such time as the training is completed.

Contractor personnel security

All contractor employees who require access to the department of veterans affairs' computer systems shall be the subject of a background investigation and must receive a favorable adjudication from the va security and investigations center (07c). The level of background security investigation shall be in accordance with va directive 0710 dated september 10, 2004 and is available at: http://www.va.gov/pubs/asp/edsdirec.asp (va handbook 0710, appendix a, and tables 1 - 3). Appropriate background investigation (bi) forms shall be provided upon contract (or task order) award (attachment 3 of sow), and are to be completed and returned to the va security and investigations center (07c) within 3 days for processing. Contractors shall be notified by 07c when the bi has been completed and adjudicated. These requirements are applicable to all sub-contractor personnel requiring the same access. If the security clearance investigation is not

completed prior to the start date of the contract, the employee shall not work on the contract while the security clearance is being processed. Work will commence as soon as the co and contractor employee receive an email message verifying that the background investigation request has been completed and the case has been initiated by the security investigations center. When the case is completed, all adjudicative paperwork will be returned to the requesting office.

The investigative history for contractor personnel working under this contract must be maintained in the databases of either the office of personnel management (opm) or the defense industrial security clearance organization (disco). .

Background investigation

The position sensitivity impact for this effort has been designated as low risk and the level of background investigation is naci.

Contractor responsibilities

The contractor shall bear the expense of obtaining background investigations. If the investigation is conducted by the office of personnel management (opm) through the va, the contractor shall reimburse the va within 30 days.

Background investigations from investigating agencies other than opm are permitted if the agencies possess an opm and defense security service certification. The vendor cage code number must be provided to the security and investigations center (07c), which shall verify the information and advise the contracting officer whether access to the computer systems can be authorized.

The contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain a u.s. Citizenship and are able to read, write, speak and understand the english language.

After contract award and prior to contract performance, the contractor shall provide the information to the cor to initiate background investigations which includes such data as ssn, dob, address, phone, and email:

The contractor, when notified of an unfavorable determination by the government, shall withdraw the employee from consideration from working under the contract. Failure to comply with the contractor personnel security requirements may result in termination of the contract for default.

Further, the contractor shall be responsible for the actions of all individuals provided to work for the 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.”

Intranet/internet

The contractor shall comply with department of veterans affairs (va) directive 6102 and va handbook 6102 (internet/intranet services).

Va directive 6102 sets forth policies and responsibilities for the planning, design, maintenance support, and any other functions related to the administration of a va internet/intranet service site or related service (hereinafter referred to as internet). This directive applies to all organizational elements in the department. This policy applies to all individuals designing and/or maintaining va internet service sites; including but not limited to full time and part time employees, contractors, interns, and volunteers. This policy applies to all va internet/intranet domains and servers that utilize va resources. This includes but is not limited to va.gov and other extensions such as, ".com, .eddo, .mil, .net, .org," and personal internet service pages managed from individual workstations.

Va handbook 6102 establishes department-wide procedures for managing, maintaining, establishing, and presenting va internet/intranet service sites or related services (hereafter referred to as "internet"). The handbook implements the policies contained in va directive 6102, internet/intranet services. This includes, but is not limited to, file transfer protocol (ftp), hypertext markup language (html), simple mail transfer protocol (smtp), web pages, active server pages (asp), e-mail forums, and list servers.

Va directive 6102 and va handbook 6102 are available at:

Internet/intranet services directive 6102
Http://www.va.gov/pubs/directives/information-resources-management-(irm)/6102d.doc
Internet/intranet services handbook 6102
Http://www.va.gov/pubs/handbooks/information-resources-management-(irm)/6102h.doc

Internet/intranet services handbook 6102 change 1 – updates va's cookie use policy, section 508 guidelines, guidance on posting of hot topics, approved warning notices, and minor editorial errors.
Http://www.va.gov/pubs/handbooks/information-resources-management-(irm)/61021h.doc

In addition, any technologies that enable a network delivered application (nda) to access or modify resources of the local machine that are outside of the browser's "sand box" are strictly prohibited. Specifically, this prohibition includes signed-applets or any activex controls delivered through a browser's session. Activex is expressly forbidden within the va while .net is allowed only when granted a waiver by the va cio *prior* to use.

Javascript is the preferred language standard for developing relatively simple interactions (i.e., forms validation, interactive menus, etc.) And applets (j2se apis and java language) for complex network delivered applications.

8. Section 508 compliance

The contractor shall comply with section 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.

In december 2000, the architectural and transportation barriers compliance board (access board), pursuant to section 508(2) (a) of the rehabilitation act amendments of 1998, established information technology accessibility standards for the federal government. Section 508(a)(1) requires that when federal departments or agencies develop, procure, maintain, or use electronic and information technology (eit), they shall ensure that the eit 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. The section 508 requirement also applies to members of the public seeking information or services from a federal department or agency.

Section 508 text is available at:
HTTP://WWW.OPM.GOV/HTML/508-TEXTOFLAW.HTM
HTTP://WWW.SECTION508.GOV/INDEX.CFM?FUSEACTION=CONTENT&ID=14

TYPE OF CONTRACT(S)

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

POINTS OF CONTACT

VA Program Manager:
Name: Gilbert Hill
Address:
Voice: 678-225-9160
Email: Gilbert.Hill@va.gov

Contracting Officer's Representative:
Name: Thomas Manning
Address:

Voice: 720-363-0357
Email: Thomas.Manning2@va.gov

Contracting Officer:
Name: Lino Vera
Address:
Voice: 512-981-4415
Email: Lino.Vera@va.gov

Contract Specialist
Name: Tommy Haire
Address:
Voice: 512-981-4457
Email: tommy.haire@va.gov