



# **PERFORMANCE WORK STATEMENT (PWS) DEPARTMENT OF VETERANS AFFAIRS**

**Office of Information & Technology  
Enterprise Program Management Office**

**LOGICARE Patient Instructions Two Factor Authentication (2FA) Compliance –  
Phase 2**

**Date: April 24, 2017  
TAC-17-44049  
PWS Version Number: 1.0**

## Contents

1.0	BACKGROUND .....	3
2.0	APPLICABLE DOCUMENTS .....	4
3.0	SCOPE OF WORK .....	7
4.0	PERFORMANCE DETAILS .....	7
4.1	PERFORMANCE PERIOD.....	7
4.2	PLACE OF PERFORMANCE.....	7
4.3	TRAVEL .....	7
5.0	SPECIFIC TASKS AND DELIVERABLES.....	7
5.1	PROJECT MANAGEMENT .....	7
5.1.1	CONTRACTOR PROJECT MANAGEMENT PLAN .....	7
5.1.2	REPORTING REQUIREMENTS .....	8
5.1.3	CONTRACTOR IMPLEMENTATION SCHEDULE .....	8
5.1.4	PRIVACY & HIPAA TRAINING .....	9
5.1.5	TECHNICAL KICKOFF MEETING .....	9
5.1.6	ONBOARDING.....	9
5.1.7	RISK MANAGEMENT .....	10
5.2	LOGICARE PATIENT INSTRUCTIONS.....	10
5.2.1	COTS PRODUCT DELIVERY .....	10
5.2.2	TESTING.....	10
5.2.3	IMPLEMENTATION .....	11
5.2.4	END USER TRAINING MATERIALS .....	11
5.2.5	WARRANTY SUPPORT .....	11
6.0	GENERAL REQUIREMENTS .....	11
6.1	ENTERPRISE AND IT FRAMEWORK.....	11
6.2	SECURITY AND PRIVACY REQUIREMENTS .....	13
6.2.1	POSITION/TASK RISK DESIGNATION LEVEL(S) .....	13
6.2.2	CONTRACTOR PERSONNEL SECURITY REQUIREMENTS .....	14
6.3	METHOD AND DISTRIBUTION OF DELIVERABLES .....	16
6.4	PERFORMANCE METRICS .....	16
6.5	FACILITY/RESOURCE PROVISIONS.....	17
6.6	GOVERNMENT FURNISHED PROPERTY .....	18
6.7	SHIPMENT OF HARDWARE OR EQUIPMENT .....	18
	ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED .....	19
	ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM	
	SECURITY/PRIVACY LANGUAGE.....	26
	VA POINTS OF CONTACT .....	32

## 1.0 BACKGROUND

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

The Cyberspace Policy Review, adopted by the President in 2011, highlighted the importance of identity management in protecting the nation's infrastructure. Homeland Security Presidential Directive-12 (HSPD-12) is a strategic initiative intended to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. HSPD-12 requires agencies to follow specific technical standards and business processes for the issuance and routine use of Federal Personal Identity Verification (PIV) smartcard credentials to verify employees' and contractors' identities. Specific benefits of the standardized credentials include secure access to federal facilities and disaster response sites, as well as multi-factor authentication, digital signature and encryption capabilities.

The majority of the federal workforce is now in possession of the credentials, and therefore agencies are in a position to aggressively step up their efforts to use the electronic capabilities of the credentials. To that end each agency is to develop and issue an implementation policy through which the agency will require the use of the PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems. All existing systems must be upgraded to use PIV credentials for authentication in accordance with NIST guidelines. Systems currently not using PIV authentication shall complete upgrades no later than April 30, 2017.

VA Identity and Access Management (IAM) provides a Single Sign-On Internal (SSOi) service that allows applications to quickly become 2FA compliant. The IAM team has been tasked with coordinating integration of VA applications which are currently NOT in compliance with the 2FA mandate. There are many paths to 2FA (IAM SSOi, AD Integrated Windows Authentication [IWA], Direct PIV). IAM is coordinating with application owners to ensure all applications have a path to 2FA.

LOGICARE Patient Instructions is a software package used by VA clinicians (e.g. nurses and providers) to deliver customized patient education and patience instructions to veterans. Uses include: emergency department discharge instructions, inpatient admission orientation, daily teaching and discharge instructions and also patient education in outpatient clinics.

## 2.0 APPLICABLE DOCUMENTS

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

1. 44 U.S.C. § 3541, “Federal Information Security Management Act (FISMA) of 2002”
2. Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements For Cryptographic Modules”
3. FIPS Pub 201-2, “Personal Identity Verification of Federal Employees and Contractors,” August 2013
4. 10 U.S.C. § 2224, “Defense Information Assurance Program”
5. Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Development (CMMI-DEV), Version 1.3 November 2010; and Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Acquisition (CMMI-ACQ), Version 1.3 November 2010
6. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
7. 42 U.S.C. § 2000d “Title VI of the Civil Rights Act of 1964”
8. VA Directive 0710, “Personnel Security and Suitability Program,” June 4, 2010, <http://www.va.gov/vapubs/>
9. VA Handbook 0710, Personnel Security and Suitability Security Program, May 2, 2016, <http://www.va.gov/vapubs>
10. VA Directive and Handbook 6102, “Internet/Intranet Services,” July 15, 2008
11. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
12. Office of Management and Budget (OMB) Circular A-130, “Managing Federal Information as a Strategic Resource,” July 28, 2016
13. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
14. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
15. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
16. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
17. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, 2012
18. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” March 10, 2015
19. VA Handbook 6500.1, “Electronic Media Sanitization,” November 03, 2008
20. VA Handbook 6500.2, “Management of Breaches Involving Sensitive Personal Information (SPI)”, October, 28, 2015
21. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring Of VA Information Systems,” February 3, 2014
22. VA Handbook 6500.5, “Incorporating Security and Privacy in System Development Lifecycle”, March 22, 2010

LOGICARE Patient Instructions Two Factor Authentication (2FA) Compliance – Phase 2  
TAC Number: TAC-17-44049

23. VA Handbook 6500.6, "Contract Security," March 12, 2010
24. VA Handbook 6500.8, "Information System Contingency Planning", April 6, 2011
25. OI&T ProPath Process Methodology (reference process maps at <http://www.va.gov/PROPATH/Maps.asp> and templates at <http://www.va.gov/PROPATH/Templates.asp>)
26. One-VA Technical Reference Model (TRM) (reference at <http://www.va.gov/trm/TRMHomePage.asp>)
27. National Institute Standards and Technology (NIST) Special Publications (SP)
28. VA Directive 6508, "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 15, 2014
29. VA Handbook 6508.1, "Procedures for Privacy Threshold Analysis and Privacy Impact Assessment," July 30, 2015
30. VA Directive 6300, Records and Information Management, February 26, 2009
31. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
32. OMB Memorandum, "Transition to IPv6", September 28, 2010
33. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015
34. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 24, 2014
35. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
36. 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
37. 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
38. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
39. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
40. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
41. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
42. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
43. NIST SP 800-157, Guidelines for Derived PIV Credentials, December 2014
44. NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
45. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014

LOGICARE Patient Instructions Two Factor Authentication (2FA) Compliance – Phase 2  
TAC Number: TAC-17-44049

46. 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>)
47. VA Memorandum, VAIQ # 7011145, VA Identity Management Policy, June 28, 2010 (reference Enterprise Architecture Section, PIV/IAM (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>)
48. IAM Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, PIV/IAM (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>)
49. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, Department of Homeland Security, October 1, 2013, [https://www.fedramp.gov/files/2015/04/TIC\\_Ref\\_Arch\\_v2-0\\_2013.pdf](https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf)
50. OMB Memorandum M-08-05, "Implementation of Trusted Internet Connections (TIC), November 20, 2007
51. OMB Memorandum M-08-23, Securing the Federal Government's Domain Name System Infrastructure, August 22, 2008
52. 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>)
53. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
54. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
55. Executive Order 13693, "Planning for Federal Sustainability in the Next Decade", dated March 19, 2015
56. Executive Order 13221, "Energy-Efficient Standby Power Devices," August 2, 2001
57. VA Directive 0058, "VA Green Purchasing Program", July 19, 2013
58. VA Handbook 0058, "VA Green Purchasing Program", July 19, 2013
59. Office of Information Security (OIS) VAIQ #7424808 Memorandum, "Remote Access", January 15, 2014, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
60. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
61. 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>
62. 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>
63. 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>
64. Epic PIV\_2\_Factor\_Authentication\_Mandate\_June\_2016

- 65. VA\_Security\_Compliance\_Epic\_VA Dir 6510 - VA Identity and Access Management
- 66. VA Enterprise Design Patterns: Privacy and Security, User Identity Authentication Version 2.0 March 2016:  
([https://www.ea.oit.va.gov/EAOIT/docs/Oct\\_2016\\_Release\\_Docs/Privacy-and-Security-User-Identity-Authentication-EDP-V1-7\\_For-Signed.pdf](https://www.ea.oit.va.gov/EAOIT/docs/Oct_2016_Release_Docs/Privacy-and-Security-User-Identity-Authentication-EDP-V1-7_For-Signed.pdf))
- 67. IAM Guidelines
  - a. VA\_IAM\_AcS Integration\_Patterns
  - b. AcS\_Common\_Business\_Rules\_Document
  - c. IAM SSOi Overview
- 68. VistA-based Applications and 2FA

### **3.0 SCOPE OF WORK**

The Contractor shall deliver, test, and implement a new two factor authentication compliant version of the LOGICARE Patient Instructions Commercial Off The Shelf (COTS) product.

### **4.0 PERFORMANCE DETAILS**

#### **4.1 PERFORMANCE PERIOD**

The period of performance shall be 4 months from the date of award.

#### **4.2 PLACE OF PERFORMANCE**

Tasks under this PWS shall be performed at Contractor facilities. The Contractor shall identify the Contractor's place of performance in their Task Execution Plan submission.

#### **4.3 TRAVEL**

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

### **5.0 SPECIFIC TASKS AND DELIVERABLES**

#### **5.1 PROJECT MANAGEMENT**

##### **5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN**

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

contract. The Contractor shall update and maintain the VA PM approved CPMP throughout the PoP.

**Deliverable:**

- A. Contractor Project Management Plan

### **5.1.2 REPORTING REQUIREMENTS**

The Contractor shall provide the COR with bi-weekly (every two weeks) 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. These reports shall reflect data as of the last day of the preceding two week period.

The bi-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. The Contractor shall monitor performance against the CPMP and report any deviations. It is expected that the Contractor will keep in communication with VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

These reports shall not be the only means of communication between the Contractor, COR and the VA Program/Project Manager to advise of performance/schedule issues and to develop strategies for addressing the issues. The Contractor shall continuously monitor performance and report any deviation from the Implementation Schedule (see paragraph 5.1.3 below) or previous bi-weekly Progress Report to the COR and VA Program/Project Manager during routine, regular communications.

**Deliverable:**

- A. Bi-Weekly Progress Report

### **5.1.3 CONTRACTOR IMPLEMENTATION SCHEDULE**

The Contractor shall deliver a Contractor Implementation Schedule showing new product completion, testing, integration, implementation at site, and warranty support. The initial baseline schedule shall be concurred upon and updated in accordance with Section B of the Delivery Order. The Contractor shall update and maintain the VA Program Manager (PM) approved schedule throughout the PoP.

**Deliverable:**

- A. Contractor Implementation Schedule



#### 5.1.4 PRIVACY & HIPAA TRAINING

The Contractor shall submit TMS Training Certificates of completion for VA Privacy and Information Security Awareness, Rules of Behavior and Health Insurance Portability and Accountability Act (HIPAA) training **for all new employees who have not yet been trained/verified**. The Contractor shall provide signed copies of the Contractor Rules of Behavior in accordance with Section 9, Training, from Appendix C of the VA Handbook 6500.6, "Contract Security". The Contractor shall submit status of VA Privacy and Information Security Awareness training for all individuals engaged on the task. For current employees who have already completed all required training, this requirement will not apply.

##### **Deliverables:**

- A. TMS Training Certificates **(if applicable as stated above)**
- B. Signed Contractor Rules of Behavior **(if applicable as stated above)**

#### 5.1.5 TECHNICAL KICKOFF MEETING

The Contractor shall hold a technical kickoff meeting within 10 business days after TO award. The Contractor shall present, for review and approval by the Government, the details of the intended approach, work plan, and project schedule for each effort. The Contractor shall specify dates, locations, agenda (shall be provided to all attendees at least five calendar days prior to the meeting), and meeting minutes (shall be provided to all attendees within three calendar days after the meeting). The Contractor shall invite the Contracting Officer (CO), Contract Specialist (CS), COR, and the VA PM.

The Contractor shall deliver the kick-off meeting package 5 (five) days after the kickoff meeting. The package shall include a work planning and delivery approach, milestone schedule, and constraints.

#### 5.1.6 ONBOARDING

The Contractor shall manage the onboarding of its staff **for all new employees who have not yet been onboarded**. Onboarding includes steps to obtain a VA network and email account, complete training, initiate background investigations, and gain physical and logical access, which may include elevated privileges to the necessary development and test environments for the various systems to be enhanced.

A single Contractor Onboarding POC shall be designated by the Contractor that tracks the onboarding status of all Contractor personnel. The Contractor Onboarding POC shall be responsible for accurate and timely submission of all required VA onboarding paperwork to the COR. The Contractor shall be responsible for tracking the status of all its staff's onboarding activities and report the status at the staff level during onboarding status meetings. The Contractor shall provide an Onboarding Status Report weekly for any staff with outstanding onboarding requests for review by the COR, VA PM and Project Manager. For current employees who have already completed the requirements, this will not apply.

**Deliverable:**

A. Onboarding Status Report (if applicable as stated above)

**5.1.7 RISK MANAGEMENT**

The Contractor shall conduct risk management of all work performed under this TO and provide input to the product Risk Management registry within Rational maintained by VA.

The Contractor shall:

1. Report, monitor, manage and mitigate risks for each respective product.
2. Assess the status of its risks on a bi-weekly basis and provide them to VA. When new risks occur which could impact testing and deployment schedule, the Contractor shall notify the COR and VA PM via email within 24 hours. Email subject line shall read "{Project Name} Risk Alert Notification."
3. Provide this information in the bi-weekly Progress Report.

**5.2 LOGICARE PATIENT INSTRUCTIONS**

The Contractor shall deliver and test a 2FA compliant version of their LOGICARE Patient Instructions COTS which utilizes SSOi integration with IAM services. The contractor will coordinate installation and implementation at all currently deployed LOGICARE Patient Instructions sites.

**5.2.1 COTS PRODUCT DELIVERY**

The Contractor shall deliver a new version of their LOGICARE Patient Instructions COTS product that provides SSOi integration with IAM services for performing authentication.

The following information is applicable to the LOGICARE 2FA – Phase 2:

- The product delivered relates to token acquisition from IAM's Secure Token Server (STS), and subsequent use of the STS-provided "SAML Token" to access VistA data from the VA's VistA Integration Adapter (VIA) technology.
- This function enables leveraging a 2FA-acquired user identity to authenticate against a VistA instance using VIA.

**5.2.2 TESTING**

The Contractor shall test and verify the COTS product in the VA environment. The Contractor shall conduct tests (e.g. integration and 2FA SSOi) prior to implementation. The Contractor shall perform remediation of the software as required to successfully comply with 2FA requirements and fully integrate the product back into the VA environment. COR/VA PM acceptance will be provided prior to production installation.

**Deliverables:**

- A. Test Results

**5.2.3 IMPLEMENTATION**

The contractor shall conduct a virtual Release Presentation/Demo to discuss the changes implemented to the product. Contractor shall identify where current installations exist and ensure that release implementation is conducted in such a way that final product is released into the correct environments. The Contractor shall hold site calls with VA staff once the product is approved for production release. The contractor will coordinate installation and implementation at all currently deployed LOGICARE Patient Instructions sites.

**Deliverables:**

- A. Release Notes

**5.2.4 END USER TRAINING MATERIALS**

The Contractor shall update their training materials, where they may exist, to assist with the training of end users of the system. Training materials are generally limited to mouse over, online help and updating the existing user manual. Examples of training material include but are not limited to: Word Documents, PDF Documents, Presentations, Wiki Pages.

The Contractor shall Update the training materials for the products that have been modified. The updates shall reflect the content and changes of the most recently deployed COTS version.

**5.2.5 WARRANTY SUPPORT**

For a period of 90 days after the final Implementation is completed the Contractor shall warrant all requirements and deliverables in the scope of this contract. Defects may be identified by the Government and its designees, to include all necessary personnel as designated by the COR. For each defect identified, the Contractor shall triage the defect, identify a resolution, and provide a plan for resolution, including timeline. Following COR approval of the plan for resolution, the Contractor shall execute the approved 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 OI&T Technical Reference Model (One-VA TRM). One-VA TRM is one component within the overall Enterprise

LOGICARE Patient Instructions Two Factor Authentication (2FA) Compliance – Phase 2  
TAC Number: TAC-17-44049

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](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](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 are set forth in OMB Memoranda M-04-04 (<http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf>), M-05-24 (<http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf>), M-11-11 (<http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf>), National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, and supporting NIST Special Publications.

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) (<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf>), M08-23 mandating Domain Name System Security (NSSEC) (<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf>), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 [https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC\\_Ref\\_Arch\\_v2-0\\_2013.pdf](https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/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.

## **6.2 SECURITY AND PRIVACY REQUIREMENTS**

### **6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)**

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

### Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low / NACI	Tier 2 / Moderate / MBI	Tier 4 / High / BI
5.1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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

#### 6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

##### Contractor Responsibilities:

- a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
- b. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the ProPath (PAL) template. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.
- c. The Contractor should coordinate with the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized. The Contractor shall bring their completed Security and Investigations Center (SIC) Fingerprint request form with them (see paragraph d.4. below) when getting fingerprints taken.
- d. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
  - 1) Optional Form 306
  - 2) Self-Certification of Continuous Service

- 3) VA Form 0710
- 4) Completed SIC Fingerprint Request Form
- e. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
- f. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via e-QIP).
- g. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
- h. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC), completed training delineated in VA Handbook 6500.6 (Appendix C, Section 9), signed "Contractor Rules of Behavior", and with a valid, operational PIV credential for PIV-only logical access to VA's network. A PIV card credential can be issued once your SAC has been favorably adjudicated and your background investigation has been scheduled by OPM. However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of OPM.
- i. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
- j. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.
- k. Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

**Deliverable:**

- A. Contractor Staff Roster

### 6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include:  
MS Word 2000/2003/2007/2010

- MS Excel 2000/2003/2007/2010
- MS PowerPoint 2000/2003/2007/2010
- MS Project 2000/2003/2007/2010
- MS Access 2000/2003/2007/2010
- MS Visio 2000/2002/2003/2007/2010
- AutoCAD 2002/2004/2007/2010
- Adobe Postscript Data Format (PDF)

### 6.4 PERFORMANCE METRICS

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

Performance Objective	Performance Standard	Acceptable Levels of Performance
A. Technical / Quality of Product or Service	<ol style="list-style-type: none"><li>1. Demonstrates understanding of requirements</li><li>2. Efficient and effective in meeting requirements</li><li>3. Meets technical needs and mission requirements</li><li>4. Provides quality services/products</li></ol>	Satisfactory or higher
B. Project Milestones and Schedule	<ol style="list-style-type: none"><li>1. Established milestones and project dates are met</li><li>2. Products completed, reviewed, delivered in accordance with the established schedule</li><li>3. Notifies customer in advance of potential problems</li></ol>	Satisfactory or higher
C. Cost & Staffing	<ol style="list-style-type: none"><li>1. Currency of expertise and staffing levels appropriate</li><li>2. Personnel possess necessary knowledge, skills and abilities to perform tasks</li></ol>	Satisfactory or higher



D. Management	1. Integration and coordination of all activities to execute effort	Satisfactory or higher
---------------	---	------------------------

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

## 6.5 FACILITY/RESOURCE PROVISIONS

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

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

This remote access may provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath, Primavera, and Remedy, including appropriate seat management and user licenses, depending upon the level of access granted. The Contractor shall utilize government-provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort. The Contractor shall not transmit, store or

otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with VA Handbook 6500, local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. The Contractor shall ensure all work is performed in countries deemed not to pose a significant security risk. For detailed Security and Privacy Requirements (additional requirements of the contract consolidated into an addendum for easy reference) refer to ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED and ADDENDUM B - VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE.

## **6.6 GOVERNMENT FURNISHED PROPERTY**

The Government will provide remote access solutions involving Citrix Access Gateway (CAG) at contractor request.

The Government will not provide IT accessories including but not limited to Mobile Wi-Fi hotspots/wireless access points, additional or specialized keyboards or mice, laptop bags, extra charging cables, extra PIV readers, peripheral devices, additional RAM, etc. The Contractor is responsible for providing these types of IT accessories in support of the TO as necessary and any VA installation required for these IT accessories shall be coordinated with the COR.

The VA COR will provide the following Government Furnished Information (GFI) for performance of this TO:

- a) Project SharePoint site access
- b) VA Account and Network Access (Virtual Private Network (VPN), or Citrix Access Gateway)
- c) VA email account
- d) All relevant project documents
- e) VA LOGICARE Site List 12-9-16b

## **6.7 SHIPMENT OF HARDWARE OR EQUIPMENT**

Not applicable.

## **ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED**

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

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

Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, unless the connection uses FIPS 140-2 (or its successor) validated encryption, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COR, CO, the PM, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

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

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

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

### **A2.0 VA Enterprise Architecture Compliance**

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

Profile (TRMSP). VA reserves the right to assess contract deliverables for EA compliance prior to acceptance.

### **A2.1. VA Internet and Intranet Standards**

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

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): [http://www1.va.gov/vapubs/viewPublication.asp?Pub\\_ID=409&FType=2](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](http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2)

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

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

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

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: <https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards> and <http://www.section508.gov/content/learn/standards>. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

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

### **A3.2. Equivalent Facilitation**

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

### **A3.3. Compatibility with Assistive Technology**

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

### **A3.4. Acceptance and Acceptance Testing**

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

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

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

### **A4.0 Physical Security & Safety Requirements:**

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

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

#### **A5.0 Confidentiality and Non-Disclosure**

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

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

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA CO will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA CO for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in

- the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA CO.
  5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
  6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
  7. Contractor must adhere to the following:
    - a. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
    - b. Controlled access to system and security software and documentation.
    - c. Recording, monitoring, and control of passwords and privileges.
    - d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
    - e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
    - f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
    - g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
    - h. Contractor does not require access to classified data.
  8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any

conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.

9. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

#### **A6.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS**

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13693, “Planning for Federal Sustainability in the Next Decade”, dated March 19, 2015; Executive Order 13221, “Energy-Efficient Standby Power Devices,” dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, Federal Energy Management Program (FEMP) designated, low standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

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

1. Provide/use ENERGY STAR products, as specified at [www.energystar.gov/products](http://www.energystar.gov/products) (contains complete product specifications and updated lists of qualifying products).
2. Provide/use the purchasing specifications listed for FEMP designated products at [https://www4.eere.energy.gov/femp/requirements/laws\\_and\\_requirements/energy\\_star\\_and\\_femp\\_designated\\_products\\_procurement\\_requirements](https://www4.eere.energy.gov/femp/requirements/laws_and_requirements/energy_star_and_femp_designated_products_procurement_requirements). The Contractor shall use the low standby power products specified at <http://energy.gov/eere/femp/low-standby-power-products>.
3. Provide/use EPEAT registered products as specified at [www.epeat.net](http://www.epeat.net). At a minimum, the Contractor shall acquire EPEAT® Bronze registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified product lists. The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists. The acquisition of Silver or Gold EPEAT registered products is encouraged over Bronze EPEAT registered products.
4. The Contractor shall use these products to the maximum extent possible without jeopardizing the intended end use or detracting from the overall quality delivered to the end user.



LOGICARE Patient Instructions Two Factor Authentication (2FA) Compliance – Phase 2  
TAC Number: TAC-17-44049

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

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

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

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

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

**B1. GENERAL**

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

**B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS**

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

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

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

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

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

### **B3. VA INFORMATION CUSTODIAL LANGUAGE**

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

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

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

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

LOGICARE Patient Instructions Two Factor Authentication (2FA) Compliance – Phase 2  
TAC Number: TAC-17-44049

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

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

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

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

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

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

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

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require Assessment and Authorization (A&A) or a Memorandum of Understanding-Interconnection Security Agreement (MOU-ISA) for

system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

#### **B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT**

Not Applicable.

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

Not Applicable.

#### **B6. SECURITY INCIDENT INVESTIGATION**

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

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

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

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

## **B7. LIQUIDATED DAMAGES FOR DATA BREACH**

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract. However, it is the policy of VA to forgo collection of liquidated damages in the event the Contractor provides payment of actual damages in an amount determined to be adequate by the agency.

b. The Contractor/Subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

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

- 1) Nature of the event (loss, theft, unauthorized access);
- 2) Description of the event, including:
  - a) date of occurrence;
  - b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
- 3) Number of individuals affected or potentially affected;
- 4) Names of individuals or groups affected or potentially affected;
- 5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
- 6) Amount of time the data has been out of VA control;
- 7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);

- 8) Known misuses of data containing sensitive personal information, if any;
- 9) Assessment of the potential harm to the affected individuals;
- 10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Breaches Involving Sensitive Personal Information*, as appropriate; and
- 11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

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

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

## **B8. SECURITY CONTROLS COMPLIANCE TESTING**

Not Applicable.

## **B9. TRAINING**

- a. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:
  - 1) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* course (TMS #10176) and complete this required privacy and security training annually; Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems.
  - 2) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access *[to be defined by*

LOGICARE Patient Instructions Two Factor Authentication (2FA) Compliance – Phase 2  
TAC Number: TAC-17-44049

*the VA program official and provided to the CO for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]*

- b. The Contractor shall provide to the CO and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 2 days of the initiation of the contract and annually thereafter, as required.
- c. Failure to complete the mandatory annual training and electronically sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

**VA POINTS OF CONTACT**

**VA Program Manager / COR:**

Name: Dick Rickard  
Organization: OI&T-Enterprise Program Management Office  
Address: 1301 Clay Street  
Oakland, CA 94612  
Email: dick.rickard@va.gov  
Phone: 503-884-6178

**Contract Specialist:**

Name: Aaron Waltersdorff  
Organization: Technology Acquisition Center - Austin  
Address: 1701 Directors Blvd. Ste. 600  
Austin, TX 78744  
Email: aaron.waltersdorff@va.gov  
Phone: 512-981-4469

**Contracting Officer:**

Name: Lateefah S. Parker  
Organization: Technology Acquisition Center - Austin  
Address: 1701 Directors Blvd. Ste. 600  
Austin, TX 78744  
Email: lateefah.parker@va.gov  
Phone: 512-981-4424