



PERFORMANCE WORK STATEMENT (PWS)  
DEPARTMENT OF VETERANS AFFAIRS  
Office of Information & Technology  
Financial Services Center

Electronic Invoicing

Date: 10 October 2019  
TAC-20-57243  
PWS Version Number: 6.0

## Contents

1.0	BACKGROUND.....	3
2.0	APPLICABLE DOCUMENTS.....	3
3.0	SCOPE OF WORK.....	7
4.0	PERFORMANCE DETAILS.....	7
4.1	PERFORMANCE PERIOD.....	7
4.2	PLACE OF PERFORMANCE.....	8
4.3	TRAVEL.....	8
5.0	SPECIFIC TASKS AND DELIVERABLES.....	8
5.1	PROJECT MANAGEMENT.....	8
5.2	CONTRACTOR PROJECT MANAGEMENT PLAN.....	8
5.3	REPORTING REQUIREMENTS.....	9
5.4	Technical kickoff meeting.....	9
6.0	E-INVOICING SOLUTION AND VENDOR EXPANSION.....	10
6.1	e-invoicing solution and services.....	10
6.2	E-INVOICING VENDOR ENROLLMENT.....	12
6.3	E-INVOICING CUSTOMER SUPPORT.....	13
7.0	E-INVOICING MAINTENANCE AND REPORTING.....	13
7.1	MAINTENANCE.....	13
7.2	REPORTING & SPEND ANALYSIS TOOL TRIAL (OPTIONAL TASK).....	13
7.3	REPORTING & SPEND ANALYSIS TOOL (OPTIONAL TASK).....	14
7.4	TRANSITION AND CONSULTING SERVICES (OPTIONAL TASK).....	14
<b>8.0</b>	<b>GENERAL REQUIREMENTS.....</b>	<b>14</b>
8.1.	ENTERPRISE AND IT FRAMEWORK.....	14
8.2.	VA TECHNICAL REFERENCE MODEL.....	14
8.3.	FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM) 15	
8.4.	INTERNET PROTOCOL VERSION 6 (IPV6).....	16
8.5.	TRUSTED INTERNET CONNECTION (TIC).....	17
8.6.	STANDARD COMPUTER CONFIGURATION.....	17
8.7.	VETERAN FOCUSED INTEGRATION PROCESS (VIP).....	18
8.8.	PROCESS ASSETT LIBRARY (PAL).....	18
8.9.	AUTHORITATIVE DATA SOURCES.....	18
8.10.	SECURITY AND PRIVACY REQUIREMENTS.....	19
8.11.	POSITION/TASK RISK DESIGNATION LEVEL(S).....	19
8.12.	CONTRACTOR PERSONNEL SECURITY REQUIREMENTS.....	20
8.13.	METHOD AND DISTRIBUTION OF DELIVERABLES.....	22
8.14.	PERFORMANCE METRICS.....	22
8.15.	FACILITY/RESOURCE PROVISIONS.....	23

## **1.0 BACKGROUND**

The mission of the Department of Veterans Affairs (VA), Office of Information & Technology (OI&T), Financial Services Center (FSC) 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 VA FSC is a Franchise Fund site authorized pursuant to the Government Management Reform Act of 1994 (Public Law 103-356). The Act authorizes designated agencies to provide certain common administrative support services on a reimbursable basis both internally and to other Government agencies. In 2006, permanent status was conferred upon the VA Franchise Fund under the "Military Quality of Life and Veterans Affairs Appropriations Act 2006," Public Law 109-114. Consequently, the VA FSC receives no federally appropriated funding and is required to market VA FSC services to customers. FSC currently offers electronic invoicing through electronic data interchange (EDI), or a third party electronic invoicing company. Approximately 95% of the 2.0 million invoices processed by the FSC annually are via e-invoicing. The current e-invoicing solution includes 450 automated integrations with high volume vendors and 45,000 web form accounts with lower volume vendors. VA-FSC objective is to reach a 98% automation rate by 2025. FSC requires services to continue and improve electronic invoicing (e-Invoicing) to improve quality, streamline business processes and reduce operating costs associated with the processing and paying of invoices.

## **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. § 3541-3549, "Federal Information Security Management Act (FISMA) of 2002"
2. "Federal Information Security Modernization Act of 2014"
3. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules"
4. FIPS Pub 199. Standards for Security Categorization of Federal Information and Information Systems, February 2004
5. FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems, March 2016
6. FIPS Pub 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013

7. 10 U.S.C. § 2224, "Defense Information Assurance Program"
8. 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
9. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
10. Public Law 109-461, Veterans Benefits, Health Care, and Information Technology Act of 2006, Title IX, Information Security Matters
11. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
12. VA Directive 0710, "Personnel Security and Suitability Program," June 4, 2010, <http://www.va.gov/vapubs/>
13. VA Handbook 0710, Personnel Security and Suitability Security Program, May 2, 2016, <http://www.va.gov/vapubs>
14. VA Directive and Handbook 6102, "Internet/Intranet Services," July 15, 2008
15. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
16. Office of Management and Budget (OMB) Circular A-130, "Managing Federal Information as a Strategic Resource," July 28, 2016
17. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
18. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
19. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended, January 18, 2017
20. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
21. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, 2012
22. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," March 10, 2015
23. VA Handbook 6500.1, "Electronic Media Sanitization," November 03, 2008
24. VA Handbook 6500.2, "Management of Breaches Involving Sensitive Personal Information (SPI)," July 28, 2016
25. VA Handbook 6500.3, "Assessment, Authorization, And Continuous Monitoring Of VA Information Systems," February 3, 2014
26. VA Handbook 6500.5, "Incorporating Security and Privacy in System Development Lifecycle", March 22, 2010
27. VA Handbook 6500.6, "Contract Security," March 12, 2010
28. VA Handbook 6500.8, "Information System Contingency Planning", April 6, 2011
29. OI&T Process Asset Library (PAL), <https://www.va.gov/process/> . Reference Process Maps at <https://www.va.gov/process/maps.asp> and Artifact templates at <https://www.va.gov/process/artifacts.asp>
30. One-VA Technical Reference Model (TRM) (reference at <https://www.va.gov/trm/TRMHomePage.aspx>)

31. VA Directive 6508, "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 15, 2014
32. VA Handbook 6508.1, "Procedures for Privacy Threshold Analysis and Privacy Impact Assessment," July 30, 2015
33. VA Handbook 6510, "VA Identity and Access Management", January 15, 2016
34. VA Directive 6300, Records and Information Management, February 26, 2009
35. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
36. NIST SP 800-37 Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach, June 5, 2014
37. NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, January 22, 2015
38. OMB Memorandum, "Transition to IPv6", September 28, 2010
39. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015
40. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 24, 2014
41. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
42. OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies, December 16, 2003
43. 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
44. 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
45. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
46. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
47. NIST SP 800-116 Rev 1, Guidelines for the Use of Personal Identity Verification (PIV) Credentials in Facility Access, June 2018
48. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
49. NIST SP 800-63-3, 800-63A, 800-63B, 800-63C, Digital Identity Guidelines, June 2017
50. NIST SP 800-157, Guidelines for Derived PIV Credentials, December 2014
51. NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
52. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014

53. 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>)
54. 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>)
55. VA Memorandum "Mandate to meet PIV Requirements for New and Existing Systems" (VAIQ# 7712300), June 30, 2015, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4846>
56. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.2, Federal Interagency Technical Reference Architectures, Department of Homeland Security, June 19, 2017, [https://www.dhs.gov/sites/default/files/publications/TIC\\_Ref\\_Arch\\_v2.2\\_2017.pdf](https://www.dhs.gov/sites/default/files/publications/TIC_Ref_Arch_v2.2_2017.pdf)
57. OMB Memorandum M-08-05, "Implementation of Trusted Internet Connections (TIC)", November 20, 2007
58. OMB Memorandum M-08-23, Securing the Federal Government's Domain Name System Infrastructure, August 22, 2008
59. 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>)
60. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
61. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
62. Executive Order 13834, "Efficient Federal Operations", dated May 17, 2018
63. Executive Order 13221, "Energy-Efficient Standby Power Devices," August 2, 2001
64. VA Directive 0058, "VA Green Purchasing Program", July 19, 2013
65. VA Handbook 0058, "VA Green Purchasing Program", July 19, 2013
66. Office of Information Security (OIS) VAIQ #7424808 Memorandum, "Remote Access", January 15, 2014, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
67. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
68. 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>
69. 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>



70. 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>
71. "Veteran Focused Integration Process (VIP) Guide 3.2", December 2018,  
<https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>
72. "VIP Release Process Guide", Version 1.4, May 2016,  
<https://www.voa.va.gov/DocumentView.aspx?DocumentID=4411>
73. "POLARIS User Guide", Version 1.9, March 2017,  
<https://www.voa.va.gov/DocumentView.aspx?DocumentID=4412>
74. VA Memorandum "Use of Personal Email (VAIQ #7581492)", April 24, 2015,  
<https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28>

### **3.0 SCOPE OF WORK**

The Contractor shall provide an e-invoicing service to support VA FSC commercial invoice processing and Veterans Benefits Administration (VBA) payments with Purchase Order (PO) and VBA Vocational Rehabilitation and Employment (VR&E) Authorizations sent to the service and invoice data automatically exported from the service to the existing VA FSC invoice processing system. The e-invoicing solution supports FSC internal and external customers, where internal customers are the VA stations creating Purchase Orders/Authorization Numbers and external customers are the vendors invoicing against those Purchase Orders/Authorization Numbers. The Contractor shall provide access to a wide network of VA vendors to streamline commercial invoice processing, and provide export, import, integration and help desk services. This PWS includes an optional task for e-invoicing support to non-VA federal customers of the FSC.

### **4.0 PERFORMANCE DETAILS**

#### **4.1 PERFORMANCE PERIOD**

The period of performance (PoP) is May 1, 2020 through April 30, 2025, plus four 12-month option periods, if exercised. In addition, if there are optional tasks that may be exercised at any time during contract performance, but will not exceed the contracts 5-year period of performance. These optional tasks will not exceed 12-months per task. Any work at the Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO).

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

Under current definitions, four are set by date:

New Year's Day	January 1
----------------	-----------

Independence Day	July 4
Veterans Day	November 11
Christmas Day	December 25

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

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

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

## **4.2 PLACE OF PERFORMANCE**

Tasks under this PWS shall be performed 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 under this effort.

## **5.0 SPECIFIC TASKS AND DELIVERABLES**

The Contractor shall perform the following:

### **5.1 PROJECT MANAGEMENT**

### **5.2 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:** Contractor Project Management Plan

### **5.3 REPORTING REQUIREMENTS**

The Contractor shall provide the Contracting Officer Representative (COR) with Monthly Progress Reports (MPR) 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 month.

The MPR 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 Information and Communication Technology (ICT) 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.

In addition to the information above, the Contractor shall include the following data in the monthly report:

- a) Number of invoices delivered
- b) Number of failed invoices with reason for failure
- c) New vendors brought into the network with status:
  - 1. Registered
  - 2. Implemented
  - 3. Ready for initial transactions
- 4. Live
- d) Log of customer issues including status and resolution
- e) Log of upcoming and completed maintenance activities

**Deliverable:** Monthly Progress Report

### **5.4 TECHNICAL KICKOFF MEETING**

The Contractor shall hold a technical kickoff meeting within 10 days after contract 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 (can be virtual), agenda (shall be provided to all attendees at least 5 calendar days prior to the meeting), and meeting minutes (shall be

provided to all attendees within 3 calendar days after the meeting). The Contractor shall invite the Contracting Officer (CO), Contract Specialist (CS), COR, and the VA PM.

## **6.0 E-INVOICING SOLUTION AND VENDOR EXPANSION**

### **6.1 E-INVOICING SOLUTION AND SERVICES**

To meet the e-invoicing needs of other Government agencies the Contractor shall provide access to an e-Invoicing network and collaborate with VA FSC Financial Operations and IT Services to properly configure and implement the Electronic Invoicing solution so that it meets the business area's needs. Such implementation may require multiple system integrations within each government agency for which one or more initial set up efforts may be required.

The Contractor shall provide an e-invoicing solution to VA FSC's commercial vendors with the following capabilities:

- a. Ability to integrate directly with all commercial accounting systems for automatic transmittal of vendor invoices and ability to ensure secured file transmittals to the VA FSC of only valid and complete invoice data as identified by the Prompt Payment Act. Any invalid, missing, or inaccurate invoice information shall be corrected prior to submission to the FSC.
- b. The Contractor shall provide invoice files to the FSC with the required invoice data fields with an accuracy rate of 99.9%. Be capable of hourly transmission (if a payload is present) to the FSC with the required invoice data in an ANSI X-12810 format to be specified by VA. Ensure transmission accuracy rate and on-time transmit rate of Electronic Invoicing data submitted exceeds a 99.9 percent rate.
- c. Follow standard data checking routines to ensure that all records sent have been received.
- d. Ability to provide a web form with online edit checks for less complicated invoice information/data to accept invoice data and export the data to the FSC.
- e. Ability to map information/data from all commercial accounting systems and export the required invoice data to VA FSC's invoicing payment processing system.
- f. Ability to accept and deliver to the VA FSC, VBA Vocational Rehabilitation and Employment invoices for benefit payments.
- g. Ability to detect and prevent duplicate invoices. The Contractor shall have in place a process to eliminate duplicate invoice submissions. FSC currently uses a combination of the purchase order/authorization number, invoice number, invoice date, and invoice amount fields to determine if an invoice is a duplicate submission. Duplicate invoices can be separated by significant time periods. Contractor's solution shall eliminate the duplicates regardless of when the original or duplicate was submitted.

- h. Provide a nationwide vendor/supplier network with an existing and extensive vendor community and the ability to support over 65,000 active vendors.
- i. Ability to process three (3) million invoices per year initially with the ability to scale up to approximately 35 million invoices per year.
- j. Ability to provide dynamic discounting functionality. Dynamic discounting is a process which allows buyers and sellers of commercial goods and services to dynamically change the payment terms—such as net 30—to accelerated payment based on a sliding discount scale. This functionality includes the ability to request early pay.
- k. Ability to receive Purchase Orders or VBA VR&E Authorizations from the VA and to provide the capability for the supplier to convert the PO or VR&E Authorization into an invoice (i.e., “PO Flip”). Ensure that invoices are validated against the appropriate Purchase Order/Authorization Number prior to delivering electronic invoices to VA FSC.
- l. Ability to receive and then deliver a Purchase Order to the vendor in accordance with the required data elements, captured during the mapping process, to the vendor’s accounting system and populating the data elements.
- m. Ability to support storage of VA-sensitive information.
- n. Compliance with Section 508 web-based access requirements.
- o. Compliance with Prompt Payment Act requirements.
- p. Provide an audit trail, which FSC can use to review the entire e-invoicing system process from receipt of invoice through the file transmittal to the FSC. The Contractor shall provide a daily audit file which includes a history of the invoice data submitted. The history shall include the date and time of the invoice data file submission, file size (bytes), the invoice count, and any missing invoices based on comparison of Contractor files transmitted to FSC files received.
- q. All client-facing resources shall be U.S. based.
- r. VA data shall not be co-mingled with other e-invoicing customer’s data.
- s. The solution shall not require software or hardware purchase for use by the commercial vendor community.
- t. All VA data shall be stored in the U.S., protected in a Tier-3 secure facility for the life of this contract.
- u. Ability to accept VA upload of invoice status data.
- v. Ability to provide invoice status to suppliers. The Contractor shall provide the capability for suppliers to obtain easy access and full visibility to relevant information relating to the processing and payment status of their invoices.
- w. The Contractor shall provide on a weekly basis to the vendor community of approximately 35,000, interactive webinars, tutorials, and on-line training during vendor onboarding and transition within 18 months in accordance with optional task Transition and Consulting Services. As the transition period progresses and as vendors become trained, the training shall then be offered on a monthly basis.
- x. The Contractor is responsible for all VA invoice data until it is successfully received by the FSC.

Note: e-invoice data is imported into the FSC Invoice Payment Processing System (IPPS). After applying the business rules, IPPS will determine the appropriate routing of the invoice data. After invoice acceptance occurs, the invoice data shall be exported to the Financial Management System (FMS) or the VA system of record for financial management for payments and VA shall prepare an invoice status upload to the e-invoicing system.

The Contractor shall provide all documentation and support required for maintenance of the existing Accreditation and Authorization (A&A) for the e-invoicing solution. A&A documentation and process requirements are found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems":

**Deliverable:** TBD

## **6.2 E-INVOICING VENDOR ENROLLMENT**

The e-invoice solution shall include all tasks necessary to enroll additional VA FSC vendors in the electronic invoicing solution. The Contractor shall, as part of their solution, conduct ongoing efforts to expand and maintain vendor community integration with the e-invoicing solution. The Contractor shall:

- a. Provide a marketing and enrollment program to ensure the participation of the FSC vendor community that includes direct oral communication with the vendors, when appropriate, to assist them with the electronic invoicing process.
- b. Perform all tasks necessary to enroll FSC vendors in the electronic invoicing solution.
- c. Implement approximately 25 new vendors per month with system integration as required.
- d. Implement approximately 25 existing vendors per month with integration changes as required.
- e. Provide approximately 2,000 web form modifications as required.
- f. Provide a process to ensure that the vendor includes the correct VA vendor identification number on invoices submitted to the FSC for payment. Vendors are established in FMS with the federal tax identification number (TIN) as the FMS vendor code. The legal name for the vendor is placed on the Vendor Name line. If there is a "doing business as" (dba) name for the location, that name is placed on Address Line 1 and on the "Vendor Name Xref" line in the FMS vendor file. If there are multiple locations for a vendor, each file is given a two-digit alternate address indicator in the Vendor Code.

The Contractor shall provide a summary of vendor integration activity in the Monthly Progress Report.

### **6.3 E-INVOICING CUSTOMER SUPPORT**

The Contractor shall:

- a. Provide telephone support to customers/vendors Monday through Friday from 8AM EST to 7PM EST.
- b. Maintain a log of issues reported by customers with status and resolution for inclusion in the Monthly Progress Report.
- c. Provide development and implementation support to review and correct test files to ensure invoice data is uniform and can be processed for 450 Integrated Solution vendors within 18 months of base year contract award.
- d. Provide tracking and prioritization procedures to ensure customer issues are resolved in a timely manner.
- e. Be responsible for Customer Support Request response time of one business day and resolution in five business days except for Integrated Solution vendors where a longer resolution period will be accepted.
- f. Track and provide, monthly, a Customer Help Desk abandoned call rate metric of 3 percent or less.

The Contractor shall provide a summary of customer support activity in the Monthly Progress Report.

## **7.0 E-INVOICING MAINTENANCE AND REPORTING**

### **7.1 MAINTENANCE**

The Contractor shall maintain the e-invoice solution. The Contractor shall provide:

- a. Software updates provided approximately every quarter, or as required.
- b. Security patches provided approximately every quarter, or as required.
- c. System administration support
- d. File backup, and disaster recovery support
- e. Notice of planned system downtime

The Contractor shall notify the VA PM/COR of changes to the VA account for review and approval before implementation. The Contractor shall provide a summary of maintenance activity in the Monthly Progress Report.

### **7.2 REPORTING & SPEND ANALYSIS TOOL TRIAL (OPTIONAL TASK)**

The Contractor shall provide a reporting and spend analysis tool to evaluate data relating to electronic purchase orders and the payment of electronic invoices on a trial basis for four (4) months. The trial analysis tool shall be used by up to 10 users. This optional task can be exercised throughout any period of performance of this contract.

**Deliverable:** Spend Analysis Tool – Trial

### **7.3 REPORTING & SPEND ANALYSIS TOOL (OPTIONAL TASK)**

The Contractor shall provide an enterprise reporting and spend analysis tool to evaluate data relating to electronic purchase orders and the payment of electronic invoices. The Contractor shall provide training to any FSC customer on tool functionalities and usage instructions and support analysis tool bug fixes and patches. The Contractor shall retain historical data for the life of this PWS, sufficient to support spend analysis throughout the PoP of this contract. This optional task can be exercised throughout any period of performance of this contract.

**Deliverable:** Spend Analysis Tool

### **7.4 TRANSITION AND CONSULTING SERVICES (OPTIONAL TASK)**

The PoP of this optional task shall be 18 months.

The Contractor shall support transition of all e-invoicing data and processing from their e-invoicing solution to an internal VA solution or another Contractor solution. The Contractor shall create a transition plan covering incumbent Contractor activity to include but not limited:

1. Migration of historical invoice data
2. Migration of historical customer information data
3. Information on automated integrations
4. Migration of webform accounts

The Contractor shall implement the transition plan and conduct parallel operations for customer accounts until successful migration to the new solution has been validated. The Contractor shall discontinue invoicing for each customer account as each migration is completed with a gradual phase-out occurring over the 18 months of this task.

**Deliverable:** Transition Plan

## **8.0 GENERAL REQUIREMENTS**

### **8.1. ENTERPRISE AND IT FRAMEWORK**

### **8.2. VA TECHNICAL REFERENCE MODEL**

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (VA TRM). The 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. Moreover, the VA TRM, which includes the Standards Profile and Product List, serves as a



technology roadmap and tool for supporting OI&T. Architecture & Engineering Services (AES) has overall responsibility for the VA TRM.

### **8.3. FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM)**

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are Personal Identity Verification (PIV) card-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), [https://www.ea.oit.va.gov/EA/OIT/VA\\_EA/Enterprise\\_Technical\\_Architecture.asp](https://www.ea.oit.va.gov/EA/OIT/VA_EA/Enterprise_Technical_Architecture.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 comply with the VA Identity, Credential, and Access Management policies and guidelines set forth in the VA Handbook 6510 and align with the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance v2.0.

The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, 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 PIV card and/or Common Access Card (CAC), as determined by the business need.

The Contractor shall ensure all Contractor delivered applications and systems conform to the specific Identity and Access Management PIV requirements set forth in the Office of Management and Budget (OMB) Memoranda M-04-04, M-05-24, M-11-11, and NIST Federal Information Processing Standard (FIPS) 201-2. 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. Contractor delivered applications and systems shall be on the FIPS 201-2 Approved Product List (APL). If the Contractor delivered application and system is not on the APL, the Contractor shall be responsible for taking the application and system through the FIPS 201 Evaluation Program.

The Contractor shall ensure all Contractor delivered applications and systems support:

1. Automated provisioning and can use enterprise provisioning service.
2. Interfacing with VA's Master Veteran Index (MVI) to provision identity attributes, if the solution relies on VA user identities. MVI is the authoritative source for VA user identity data.
3. The VA defined unique identity (Secure Identifier [SEC ID] / Integrated Control Number [ICN]).
4. Multiple authenticators for a given identity and authenticators at every Authenticator Assurance Level (AAL) appropriate for the solution.
5. Identity proofing for each Identity Assurance Level (IAL) appropriate for the solution.
6. Federation for each Federation Assurance Level (FAL) appropriate for the solution, if applicable.
7. Two-factor authentication (2FA) through an applicable design pattern as outlined in VA Enterprise Design Patterns.
8. A Security Assertion Markup Language (SAML) implementation if the solution relies on assertion based authentication. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST SP 800-63-3 guidelines.
9. Authentication/account binding based on trusted Hypertext Transfer Protocol (HTTP) headers if the solution relies on Trust based authentication.
10. Role Based Access Control.
11. Auditing and reporting capabilities.
12. Compliance with VAIQ# 7712300 Mandate to meet PIV requirements for new and existing systems.

<https://www.voa.va.gov/DocumentView.aspx?DocumentID=4846>

The required Assurance Levels for this specific effort are Identity Assurance Level 3, Authenticator Assurance Level 3, and Federation Assurance Level 3.

#### **8.4. INTERNET PROTOCOL VERSION 6 (IPV6)**

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://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov\\_docs/transiti on-to-ipv6.pdf](https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/transiti on-to-ipv6.pdf)). IPv6 technology, in accordance with the USGv6 Profile, NIST Special Publication (SP) 500-267

(<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-267.pdf>), the Technical Infrastructure for USGv6 Adoption (<https://www.nist.gov/programs->

[projects/usgv6-program](https://www.va.gov/projects/usgv6-program)), and the NIST SP 800 series applicable compliance (<https://csrc.nist.gov/publications/sp>) 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>.

#### **8.5. TRUSTED INTERNET CONNECTION (TIC)**

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/y2008/m08-05.pdf>), M08-23 mandating Domain Name System Security (NSSEC) (<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/y2008/m08-23.pdf>), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 [https://www.dhs.gov/sites/default/files/publications/TIC\\_Ref\\_Arch\\_v2.2\\_2017.pdf](https://www.dhs.gov/sites/default/files/publications/TIC_Ref_Arch_v2.2_2017.pdf).

#### **8.6. STANDARD COMPUTER CONFIGURATION**

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 Office 365 ProPlus. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Windows 10. However, Windows 10 is not the VA standard yet and is currently approved for limited use during its rollout. We are in-process of this rollout and making Windows 10 the standard for OI&T. Upon the release approval of Windows 10 as the VA standard, Windows 10 will supersede 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 with switches for silent and unattended installation 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) and Defense Information

Systems Agency (DISA) Secure Technical Implementation Guide (STIG) specific to the particular client operating system being used.

### **8.7. VETERAN FOCUSED INTEGRATION PROCESS (VIP)**

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

### **8.8. PROCESS ASSETT LIBRARY (PAL)**

The Contractor shall perform their duties consistent with the processes defined in the OIT Process Asset Library (PAL). The PAL scope includes the full spectrum of OIT functions and activities, such as VIP project management, operations, service delivery, communications, acquisition, and resource management. PAL serves as an authoritative and informative repository of searchable processes, activities or tasks, roles, artifacts, tools and applicable standards and guides to assist the OIT workforce, Government and Contractor personnel. The Contractor shall follow the PAL processes to ensure compliance with policies and regulations and to meet VA quality standards. The PAL includes the contractor onboarding process consistent with Section 6.2.2 and can be found at [https://www.va.gov/PROCESS/artifacts/maps/process\\_CONB\\_ext.pdf](https://www.va.gov/PROCESS/artifacts/maps/process_CONB_ext.pdf). The main PAL can be accessed at [www.va.gov/process](http://www.va.gov/process).

### **8.9. AUTHORITATIVE DATA SOURCES**

The VA Enterprise Architecture Repository (VEAR) is one component within the overall Enterprise Architecture (EA) that establishes the common framework for data taxonomy for describing the data architecture used to develop, operate, and maintain enterprise applications. The Contractor shall comply with the department's Authoritative Data Source (ADS) requirement that VA systems, services, and processes throughout the enterprise shall access VA data solely through official VA ADSs where applicable, see below. The Information Classes which compose each ADS are located in the VEAR, in the Data & Information domain. The Contractor shall ensure that all delivered applications and system solutions support:

1. Interfacing with VA's Master Veteran Index (MVI) to provision identity attributes, if the solution relies on VA user identities. MVI is the authoritative source for VA user identity data.

2. Interfacing with Capital Asset Inventory (CAI) to conduct real property record management actions, if the solution relies on real property records data. CAI is the authoritative source for VA real property record management data.
3. Interfacing with electronic Contract Management System (eCMS) for access to contract, contract line item, purchase requisition, offering vendor and vendor, and solicitation information above the micro-purchase threshold, if the solution relies on procurement data. ECMS is the authoritative source for VA procurement actions data.
4. Interfacing with HRSmart Human Resources Information System to conduct personnel action processing, on-boarding, benefits management, and compensation management, if the solution relies on personnel data. HRSmart is the authoritative source for VA personnel information data.
5. Interfacing with Vet360 to access personal contact information, if the solution relies on VA Veteran personal contact information data. Vet360 is the authoritative source for VA Veteran Personal Contact Data.
6. Interfacing with VA/Department of Defense (DoD) Identity Repository (VADIR) for determining eligibility for VA benefits under Title 38, if the solution relies on qualifying active duty military service data. VADIR is the authoritative source for Qualifying Active Duty military service in the VA.

#### 8.10. SECURITY AND PRIVACY REQUIREMENTS

*It has been determined that protected health information may be disclosed or accessed and a signed Business Associate Agreement (BAA) shall be required. The Contractor shall adhere to the requirements set forth within the BAA, referenced in Section D of the contract, and shall comply with VA Directive 6066.*

#### 8.11. POSITION/TASK RISK DESIGNATION LEVEL(S)

In accordance with VA Handbook 0710, Personnel Security and Suitability Program, the position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the PWS are:

*(List PWS Task Section Numbers for this effort (Subsections only as required) in the first column. Double click on the selection box in the appropriate Position Risk Designation column to indicate the proper Risk Designation associated with each task based upon the PDT tool results.)*

#### Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input 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.

#### **8.12. 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 PAL template artifact. 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: Contractor Staff Roster

### 8.13. 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).

### 8.14. 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
Technical / Quality of Product or Service	Demonstrates understanding of requirements Efficient and effective in meeting requirements Meets technical needs and mission requirements Provides quality services/products	Satisfactory or higher
Project Milestones and Schedule	Established milestones and project dates are met Products completed, reviewed, delivered in accordance with the established schedule Notifies customer in advance of potential problems	Satisfactory or higher
Cost & Staffing	Currency of expertise and staffing levels appropriate Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
Management	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. <VERIFY next statement and remove if not using the assessment > A Performance Based Service Assessment will be used by the COR in accordance with the QASP to assess Contractor performance.

#### **8.15. FACILITY/RESOURCE PROVISIONS**

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

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

VA 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, PAL, 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 **Error! Reference source not found.** and ADDENDUM B - VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE.

DRAFT