

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30				1. REQUISITION NO. 116-16-2-7662-0011		PAGE 1 OF 47	
2. CONTRACT NO. NNG15SD41B		3. AWARD/EFFECTIVE DATE 3/23/2016		4. ORDER NO. VA118-16-F-0918		5. SOLICITATION NUMBER VA118-16-Q-1015	
7. FOR SOLICITATION INFORMATION CALL:		a. NAME Amanda J. Bleses Amanda.Bleses@va.gov		b. TELEPHONE NO. (No Collect Calls) 732-795-1054		8. OFFER DUE DATE/LOCAL TIME	
9. ISSUED BY Department of Veterans Affairs Technology Acquisition Center 23 Christopher Way Eatontown NJ 07724				10. THIS ACQUISITION IS <input type="checkbox"/> UNRESTRICTED OR <input type="checkbox"/> SET ASIDE: _____ % FOR: <input type="checkbox"/> SMALL BUSINESS <input type="checkbox"/> WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM NAICS: 541519 <input type="checkbox"/> HUBZONE SMALL BUSINESS <input type="checkbox"/> EDWOSB <input type="checkbox"/> SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS <input type="checkbox"/> 8(A) SIZE STANDARD: 150 Employees			
11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED <input type="checkbox"/> SEE SCHEDULE		12. DISCOUNT TERMS		13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700) <input type="checkbox"/>		13b. RATING N/A	
15. DELIVER TO See Delivery Schedule				16. ADMINISTERED BY Department of Veterans Affairs Technology Acquisition Center 23 Christopher Way Eatontown NJ 07724			
17a. CONTRACTOR/OFFEROR CODE 6ZQW0		FACILITY CODE		18a. PAYMENT WILL BE MADE BY Department of Veterans Affairs Technology Acquisition Center Financial Services Center PO Box 149971 Austin TX 78714-8971			
VETERAN INFORMATION TECHNOLOGIES, LLC		5475 MARK DABLING BOULEVARD SUITE 300		COLORADO SPRINGS CO 80918		TELEPHONE NO. _____ DUNS: 079129400DUNS+4: _____	
17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER <input type="checkbox"/>				18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED <input type="checkbox"/> SEE ADDENDUM			
19. ITEM NO.		20. SCHEDULE OF SUPPLIES/SERVICES		21. QUANTITY		22. UNIT	
						23. UNIT PRICE	
						24. AMOUNT	
		Title: International Business Machines (IBM) Kenexa Evolution Learning Content Management System (LCMS) Professional Support Services & Software Licenses Alternate POC: Robert Kirzow Phone: (732) 795-1017 Email: Robert.Kirzow@va.gov Type of Contract: Firm-Fixed-Price PO # 116-S65748 Quote #AAAQ30318 See Section B.2 for a list of software and services. The details of this order shall be delivered in accordance with the Product Description (PD) found in Section B.3 of this delivery order. (Use Reverse and/or Attach Additional Sheets as Necessary)					
25. ACCOUNTING AND APPROPRIATION DATA 116-3660167-7662-198040-2510 T0C232S0A				26. TOTAL AWARD AMOUNT (For Govt. Use Only) \$493,622.44			
<input type="checkbox"/> 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA <input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED.				<input checked="" type="checkbox"/> 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA <input type="checkbox"/> ARE <input checked="" type="checkbox"/> ARE NOT ATTACHED			
<input type="checkbox"/> 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN _____ COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED				<input type="checkbox"/> 29. AWARD OF CONTRACT: REF. _____ OFFER DATED _____ YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN IS ACCEPTED AS TO ITEMS:			
30a. SIGNATURE OF OFFEROR/CONTRACTOR				31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER) <i>Robert Kirzow</i>			
30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT)		30c. DATE SIGNED		31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT) Robert Kirzow Contracting Officer		31c. DATE SIGNED 3/23/2016	

A.2 GOVERNING LAW

Federal law and regulations, including the Federal Acquisition Regulations (FAR), shall govern this Contract/Order. Commercial license agreements may be made a part of this Contract/Order but only if both parties expressly make them an addendum hereto. If the commercial license agreement is not made an addendum, it shall not apply, govern, be a part of or have any effect whatsoever on the Contract/Order; this includes, but is not limited to, any agreement embedded in the computer software (clickwrap), any agreement that is otherwise delivered with or provided to the Government with the commercial computer software or documentation (shrinkwrap), or any other license agreement otherwise referred to in any document. If a commercial license agreement is made an addendum, only those provisions addressing data rights regarding the Government's use, duplication and disclosure of data (*e.g.*, restricted computer software) are included and made a part of this Contract/Order, and only to the extent that those provisions are not duplicative or inconsistent with Federal law, Federal regulation, the incorporated FAR clauses and the provisions of this Contract/Order; those provisions in the commercial license agreement that do not address data rights regarding the Government's use, duplication and disclosure of data shall not be included or made a part of the Contract/Order. Federal law and regulation including, without limitation, the Contract Disputes Act (41 U.S.C. § 7101 *et seq.*), the Anti-Deficiency Act (31 U.S.C. § 1341 *et seq.*), the Competition in Contracting Act (41 U.S.C. § 3301 *et seq.*), the Prompt Payment Act (31 U.S.C. § 3901 *et seq.*), Contracts for Data Processing or Maintenance (38 USC § 5725), and FAR clauses 52.212-4, 52.227-14, 52.227-19 shall supersede, control, and render ineffective any inconsistent, conflicting, or duplicative provision in any commercial license agreement. In the event of conflict between this Clause and any provision in the Contract/Order or the commercial license agreement or elsewhere, the terms of this Clause shall prevail. Claims of patent or copyright infringement brought against the Government as a party shall be defended by the U.S. Department of Justice (DOJ). 28 U.S.C. § 516. At the discretion of DOJ, the Contractor may be allowed reasonable participation in the defense of the litigation. Any additional changes to the Contract/Order must be made by contract/order modification (Standard Form 30) and shall only be effected by a warranted Contracting Officer. Nothing in this Contract/Order or any commercial license agreement shall be construed as a waiver of sovereign immunity.

Table of Contents

SECTION A..... 1

 A.1 SF 1449 SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS..... 1

 A.2 GOVERNING LAW..... 2

SECTION B - CONTINUATION OF SF 1449 BLOCKS..... 4

 B.1 CONTRACT ADMINISTRATION DATA..... 4

 B.2 PRICE SCHEDULE..... 5

 B.3 PERFORMANCE WORK STATEMENT 10

SECTION C - CONTRACT CLAUSES 45

 C.1 NASA SEWP V RFQ INTRODUCTORY LANGUAGE 45

 C.2 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)..... 45

 C.3 VAAR 852.203-70 COMMERCIAL ADVERTISING (JAN 2008) 45

 C.4 VAAR 852.232-72 ELECTRONIC SUBMISSION OF PAYMENT REQUESTS (NOV 2012)..... 46

 C.5 VAAR 852.237-70 CONTRACTOR RESPONSIBILITIES (APR 1984)..... 47

 C.6 VAAR 852.246-71 INSPECTION (JAN 2008)..... 47

SECTION B - CONTINUATION OF SF 1449 BLOCKS

B.1 CONTRACT ADMINISTRATION DATA

(continuation from Standard Form 1449, block 18A.)

1. Contract Administration: All contract administration matters will be handled by the following individuals:

a. CONTRACTOR: Veteran Information Technologies, LLC
5475 Mark Dabling Blvd, Suite 320
Colorado Springs, CO 80918

b. GOVERNMENT: Contracting Officer 0010B
Department of Veterans Affairs
Technology Acquisition Center
23 Christopher Way
Eatontown NJ 07724

2. CONTRACTOR REMITTANCE ADDRESS: All payments by the Government to the contractor will be made in accordance with:

- 52.232-34, Payment by Electronic Funds Transfer—Other Than System For Award Management, or
 52.232-36, Payment by Third Party

3. INVOICES: Invoices shall be submitted in arrears:

- a. Quarterly
b. Semi-Annually
c. Other upon acceptance of deliverables set forth in B.2, Price Schedule

4. GOVERNMENT INVOICE ADDRESS: All Invoices from the contractor shall be submitted electronically in accordance with VAAR Clause 852.232-72 Electronic Submission of Payment Requests.

Department of Veterans Affairs
Technology Acquisition Center
Financial Services Center
PO Box 149971
Austin TX 78714-8971

B.2 PRICE SCHEDULE

Base Period: March 30, 2016 through March 29, 2017					
Contract Line Item Number (CLIN)	CLIN Description	QTY	Unit	Unit Price	Total Price
0001	<p>Project Management shall be provided in accordance with (IAW) Performance Work Statement (PWS) paragraph 5.1.</p> <p>This FFP CLIN includes all labor, material, and other costs required for the successful completion of the services detailed in PWS paragraph 5.1 and all its subparagraphs.</p> <p>The cost of this line item including labor and all associated deliverables shall be allocated to CLINs 0002 through 0003.</p> <p>Period of Performance shall be March 30, 2016 through March 29, 2017.</p>	12	MO	\$ 5,502.84	\$ 66,034.08
0001AA	<p>Contractor Project Management Plan IAW PWS paragraph 5.1.1.</p> <p>Due 30 days after contract award (DAC) and updated monthly thereafter.</p> <p>Electronic submission to: VA PM and COR.</p> <p>Inspection: destination</p> <p>Acceptance: destination</p>	1	LO	NSP	NSP

0001AB	<p>Bi-Weekly PD Status Report IAW PWS paragraph 5.1.2.</p> <p>Due Two weeks after contract award and updated bi-weekly on Wednesdays thereafter.</p> <p>Electronic Submission to: VA PM and COR.</p> <p>Inspection/Acceptance/FOB: Destination</p>	1	LO	NSP	NSP
0001AC	<p>VA Privacy and Information Security Training Certificates IAW PWS paragraph 5.1.3</p> <p>Due five days after completion of training.</p> <p>Electronic Submission to: VA PM and COR.</p> <p>Inspection/Acceptance/FOB: Destination</p>	1	LO	NSP	NSP
0001AD	<p>Kickoff Meeting IAW paragraph 5.1.4.</p> <p>This meeting shall be held within 10 calendar DAC.</p>	1	EA	NSP	NSP
0001AE	<p>Kickoff Meeting Agenda IAW paragraph 5.1.4.</p> <p>Due ten DAC. Electronic Submission to: VA PM and COR.</p> <p>Inspection/Acceptance/FOB: Destination</p>	1	LO	NSP	NSP
0001AF	<p>Kickoff Meeting Presentation IAW paragraph 5.1.4</p> <p>Due 10 DAC</p> <p>Electronic Submission to: VA PM and COR.</p>	1	LO	NSP	NSP

	Inspection/Acceptance/FOB: Destination				
0001AG	Kickoff Meeting Final (Revised) Presentation IAW paragraph 5.1.4 Due 20 DAC Electronic Submission to: VA PM and COR. Inspection/Acceptance/FOB: Destination	1	LO	NSP	NSP
0002	LCMS Software Release Management The cost of this line item including labor, material and other costs required for the successful completion of the services detailed in PWS paragraph 5.2.				
0002AA	VA-Specific Delta Document (with each Release) IAW PWS paragraph 5.2. Due 10 days after announcement of Release Electronic Submission to: VA PM and COR. Inspection/Acceptance/FOB: Destination	4	EA	\$ 8,318.04	\$ 33,272.16
0002AB	Implementation Recommendation Document (with each Release) IAW PWS paragraph 5.2. Due 10 days after Delta Demonstration Electronic Submission to: VA PM and COR. Inspection/Acceptance/FOB: Destination	4	EA	\$ 8,318.04	\$ 33,272.16
0003	LCMS RELEASE-SPECIFIC IMPLEMENTATION SUPPORT The cost of this line item including labor, material and other costs required for the successful completion				

	of the services detailed in PWS paragraph 5.3 and all of its subparagraphs.				
0003AB-1	Technical Workshop Agenda IAW paragraph 5.3.1 Due one week prior to the workshop. Inspection/Acceptance/FOB: Destination	1	EA	\$ 7,960.82	\$ 7,960.82
0003AB-2	Technical Workshop Support Workshop Minutes IAW paragraph 5.3.1 Due 5 days after Workshop occurs Electronic Submission to: VA PM and COR Inspection/Acceptance/FOB: Destination	4	EA	\$ 5,715.46	\$ 22,861.84
0003AC	Implementation Plan IAW paragraph 5.3.2 Due 10 days after Workshop occurs Electronic Submission to: VA PM and COR Inspection/Acceptance/FOB: Destination	4	EA	\$3,801.80	\$15,207.20
0003AD	Roll Back Plan IAW paragraph 5.3.2 Due 10 days after Workshop occurs Electronic Submission to: VA PM and COR Inspection/Acceptance/FOB: Destination	4	EA	\$ 3,801.80	\$ 15,207.20
0003AE	Updated Software Design Document (SDD) IAW paragraph 5.3.3 Due 10 days after UAT complete Electronic Submission to: VA PM and COR Inspection/Acceptance/FOB: Destination	1	EA	\$ 23,168.04	\$ 23,168.04

0003AF	<p>Revised Extension Code IAW PWS paragraph 5.3.3</p> <p>Due 10 days after UAT complete</p> <p>Electronic Submission to: VA PM and COR.</p> <p>Inspection/Acceptance/FOB: Destination</p>	1	EA	\$ 18,677.32	\$ 18,677.32
0004	<p>LCMS TECHNICAL INTERCHANGE MEETINGS & TECHNICAL SUPPORT</p> <p>The cost of this line item including labor, material and other costs required for the successful completion of the services detailed in PWS paragraph 5.4.</p>				
0004AA	<p>Technical Interchange Meeting Report Email IAW PWS paragraph 5.4</p> <p>Due one week after meeting occurrence</p> <p>Electronic Submission to: VA PM and COR.</p> <p>Inspection/Acceptance/FOB: Destination</p>	1	LO	\$ 7,960.82	\$ 7,960.82
0005	<p>280 LCMS Authorizing Licenses (280 Authors) IAW PWS paragraph 5.5</p> <p>Electronic Submission to: VA PM and COR.</p> <p>Inspection/Acceptance/FOB: Destination</p>	1	LOT	\$ 250,000.80	\$ 250,000.80
	Total Order Price				\$ 493,622.44

B.3 PERFORMANCE WORK STATEMENT

DEPARTMENT OF VETERANS AFFAIRS



Office of Information & Technology

Product Development

Learning Content Management System (LCMS) Support Services and Licenses

Date: February 18, 2016

TAC-16-33118

PWS Version Number: 1.14

1.0 BACKGROUND

The mission of the Department of Veterans Affairs (VA), Office of Information & Technology (OI&T), Product Development (PD) 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 and licenses to those responsible for providing care to the Veterans at the point-of-care as well as throughout all the points of the Veterans' health care in an effective, timely, and compassionate manner. VA depends on Information Management/Information Technology (IM/IT) systems to meet mission goals.

VA has been using the International Business Machines (IBM) Kenexa Evolution Learning Content Management System (LCMS) since 2006. The LCMS is an object-based learning content development environment which offers complete content reusability, personalization, enterprise content management capability, and multi-modal output (Web, CD, Word, mobile, etc.) to support the consolidation of all training initiatives. It also ensures all content is Section 508 conformant prior to publication.

The LCMS is currently hosted at a VA site in St. Louis, Missouri. VA's goal is to continue its access to the LCMS so that it can maintain the number of VA entities producing content on that platform. This accomplishes efficiencies across VA and adds greater assurance that VA and Federal requirements are met, in addition to providing a number of other benefits to VA such as:

1. Providing content developers across VA with an integrated web-based standardized content development tool whose products are operable in the VA Talent Management System (TMS)
2. Allowing developers to quickly develop content objects and courses using any combination of new material and existing content objects (in all media forms)
3. Reducing the time to produce online courses, enabled through the use of:
 - a. Development templates
 - b. Section 508 compliance review features
 - c. Support services for using the LCMS
 - d. Greater data integration with TMS
 - e. Real time collaboration and multiple work streams which compresses time and cost of development
4. Enabling existing online course components (Sharable Content Objects (SCOs)) to be repurposed by developers to use or modify and combine with newly created SCOs to form online courses
5. Allowing the development of content at varying levels of granularity making the storage and retrieval of very specific components of content readily available to developers and to online course users for real-time, ad-hoc performance support
6. Allowing the use of existing reports and the creation of custom reports as they relate to content and usage including automatic notifications such as course lifecycle information
7. Providing a common development tool for developers across VA to:
 - a. Promote community of practice collaboration
 - b. Eliminate decentralized acquisition of content development software of various types across VA

2.0 APPLICABLE DOCUMENTS

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

1. 44 U.S.C. § 3541, “Federal Information Security Management Act (FISMA) of 2002”
2. Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements For Cryptographic Modules”
3. FIPS Pub 201-2, “Personal Identity Verification of Federal Employees and Contractors,” August 2013
4. 10 U.S.C. § 2224, "Defense Information Assurance Program"
5. Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Development (CMMI-DEV), Version 1.3 November 2010; and Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Acquisition (CMMI-ACQ), Version 1.3 November 2010
6. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
7. **42 U.S.C. § 2000d** “Title VI of the Civil Rights Act of 1964”
8. VA Directive 0710, “Personnel Suitability and Security Program,” June 4, 2010, <http://www1.va.gov/vapubs/>
9. VA Handbook 0710, Personnel Suitability and Security Program, September 10, 2004, <http://www1.va.gov/vapubs/>
10. VA Directive and Handbook 6102, “Internet/Intranet Services,” July 15, 2008
11. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
12. Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources,” November 28, 2000
13. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
14. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
15. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
16. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
17. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, , 2012
18. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” September 20, 2012
19. VA Handbook 6500.1, “Electronic Media Sanitization,” March 22, 2010
20. VA Handbook 6500.2, “Management of Data Breaches Involving Sensitive Personal Information (SPI)”, January 6, 2012
21. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring Of VA Information Systems,” February 3, 2014
22. VA Handbook, 6500.5, “Incorporating Security and Privacy in System Development Lifecycle” March 22, 2010
23. VA Handbook 6500.6, “Contract Security,” March 12, 2010
24. Project Management Accountability System (PMAS) portal (reference <https://www.voa.va.gov/pmas/>)
25. OI&T ProPath Process Methodology (reference <https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=27>) NOTE: In the event of a conflict, OI&T ProPath takes precedence over other processes or methodologies.
26. 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, VA Privacy Impact Assessment, October 3, 2008*
29. *VA Directive 6300, Records and Information Management, February 26, 2009*
30. *VA Handbook, 6300.1, Records Management Procedures, March 24, 2010*
31. *OMB Memorandum, “Transition to IPv6”, September 28, 2010*

32. *VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, February 17, 2011*
33. *VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 20, 2014*
34. *OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006*
35. *OMB Memorandum 05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005*
36. *OMB memorandum M-11-11, “Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011*
37. *OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008*
38. *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011*
39. *NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008*
40. *OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007*
41. *NIST SP 800-63-2, Electronic Authentication Guideline, August 2013*
42. *Draft NIST Special Publication 800-157, Guidelines for Derived PIV Credentials, March 2014*
43. *NIST Special Publication 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012*
44. *Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014*
45. *VA Memorandum, VAIQ #7100147, Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12), April 29, 2011 (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>)*
46. *VA Memorandum, VAIQ # 7011145, VA Identity Management Policy, June 28, 2010 (reference Enterprise Architecture Section, PIV/IAM (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>))*
47. *IAM Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, PIV/IAM (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>))*
48. *Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, October 1, 2013*
49. *OMB Memorandum M-08-05, “Implementation of Trusted Internet Connections (TIC), November 20, 2007*
50. *OMB Memorandum M-08-23, Securing the Federal Government’s Domain Name System Infrastructure, August 22, 2008*
51. *VA Memorandum, VAIQ #7497987, Compliance – Electronic Product Environmental Assessment Tool (EPEAT) – IT Electronic Equipment, August 11, 2014 (reference Document Libraries, EPEAT/Green Purchasing Section, <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=552>)*
52. *Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007*
53. *Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005*

54. *Executive Order 13514, "Federal Leadership in Environmental, Energy, and Economic Performance," October 5, 2009*
55. *Executive Order 13423, "Strengthening Federal Environmental, Energy, and Transportation Management," January 24, 2007*
56. *Executive Order 13221, "Energy-Efficient Standby Power Devices," August 2, 2001*
57. *VA Directive 0058, "VA Green Purchasing Program", July 19, 2013*
58. *VA Handbook 0058, "VA Green Purchasing Program", July 19, 2013*
59. *Aviation Industry Computer-based Training Committee (AICC) Web-Based Computer Managed Instruction Systems (CMI) Guideline (AGR-010), <https://github.com/ADL-AICC/AICC-Document-Archive/releases/tag/AllPubsAllVers>*
60. *Sharable Content Object Reference Model (SCORM), <http://www.adlnet.gov/>*

3.0 SCOPE OF WORK

The Contractor shall provide professional support above and beyond the services which are available from Kenexa's standard license maintenance support. This work shall include software release management support, release-specific implementation support, and technical support. The contractor shall also provide brand name IBM Kenexa LCMS software licenses as required.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance shall be March 30, 2016 – March 29, 2017.

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.

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

5.1.1 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 Project Manager (PM) approved CPMP throughout the period of performance.

Deliverable:

- A. Contractor Project Management Plan

5.1.2 REPORTING REQUIREMENTS

The Contractor shall deliver Bi-Weekly (every two weeks) Product Development (PD) Status Reports. These reports shall provide accurate, timely, and complete project information supporting PD reporting Requirements. The Bi-Weekly PD Status Report shall include the following data elements:

- a. Project Name and Contract Name
- b. Overview and description of the Contract
- c. Overall high level assessment of Contract progress
- d. All work in-progress and completed during the reporting period
- e. Identification of any Contract related issues uncovered during the reporting period and especially highlight those areas with a high probability of impacting schedule, cost, or performance goals and their likely impact on schedule, cost, or performance goals
- f. Explanations for any unresolved issues, including possible solutions and any actions required of the Government and/or Contractor to resolve or mitigate any identified issue, including a plan and timeframe for resolution

- g. Status on previously identified issues, actions taken to mitigate the situation and/or progress made in rectifying the situation
- h. Work planned for the subsequent four reporting periods, when applicable
- i. Current Contract schedule overlaid on original Contract schedule showing any delays or advancement in schedule
- j. Current definition of user requirements / function points overlaid over the original function points and the last reported function points to specifically identify changes in the function points to be delivered since the previous report
- k. Current expenditures overlaid over the original budget showing any deviations in the actual expenditures versus the original budget and versus the current budget for Cost and Time and Materials type contracts. For Firm Fixed Priced efforts provide expenditures based upon your proposed spend plan.
- l. Workforce staffing data showing all Contractor personnel performing on the effort during the current reporting period. After the initial labor baseline is provided, each Bi-Weekly PD Status Report shall identify any changes in staffing identifying each person who was added to the contract or removed from the contract.
- m. Original schedule of deliverables and the corresponding deliverables made during the current reporting period

These reports shall not be the only means of communication between the Contractor, Contracting Officer's Representative (COR), and the 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 CPMP or previous Bi-Weekly PD Status Report to the COR and Program/Project Manager during routine, regular communications.

Deliverable:

- A. Bi-Weekly PD Status Report

5.1.3 PRIVACY TRAINING

The Contractor shall submit status of VA Privacy and Information Security Awareness training for all individuals engaged on the task. The status reporting shall identify; a single Contractor Security Point of Contact POC, the names of all personnel engaged on the task, their initial training date for VA Privacy and Information Security training, and their next required training date. This information shall be submitted as part of the Bi-Weekly PD Status Report.

The Contractor shall submit VA Privacy and Information Security training certificates in accordance with Section 9, Training, from Appendix C of the VA Handbook 6500.6, "Contract Security."

Deliverable:

- A. VA Privacy and Information Security Training Certificates

5.1.4 KICK-OFF MEETING

The Contractor shall conduct a virtual technical kick-off meeting with the VA PM and COR and appropriate VA staff. This meeting shall be held within ten calendar days after award.

The Contractor shall provide a technical Kick-off Meeting Agenda with the conference call audio/video information and the topics to be presented. The Kick-off Presentation shall address post award topics, Contractor's POCs, and approach for meeting PWS requirements. The Contractor shall update the Kick-off Meeting Presentation with the results of the discussions and decisions made during the meeting (i.e., meeting minutes) and shall deliver the Final Presentation.

Deliverables:

- A. Kick-off Meeting Agenda
- B. Kick-off Presentation
- C. Kick-off Meeting Final Presentation

5.2 LCMS SOFTWARE RELEASE MANAGEMENT SUPPORT

Throughout the year, Kenexa usually provides four major upgrades to the base version of the Evolution LCMS product to all licensees. Between upgrades, Kenexa may also release patches to fix issues or bugs. Typically, VA only implements one major version upgrade per year, and only those patches that directly impact VA collectively, upgrades and patches are referred to as "releases" in this document).

The Contractor shall create a cumulative VA-Specific "Delta" Document which lists the differences between VA's current version of LCMS, including any revised requirements, and the features available and modifications made in the latest release. For each successive Release made available by Kenexa, this Delta Document shall be updated to reflect the addition of the latest release deltas.

The Contractor shall hold a virtual meeting with the VA PM and COR in which, using the VA-Specific Delta Document as a guide, they shall demonstrate all the different features and configuration options available for the latest as well as all prior non-implemented Releases.

The Contractor shall perform an analysis of the effect of the Release on VA's environment, extensions (VA-specific customizations), procedures, policies, and processes and the value of the deltas and provide an Implementation Recommendation Document listing the pros and cons of implementing versus not implementing the latest release.

Deliverables:

- A. VA-Specific Delta Document (with each Release)
- B. Implementation Recommendation Document (with each Release)

5.3 LCMS RELEASE-SPECIFIC IMPLEMENTATION SUPPORT

Upon Government decision to implement a Release, the Contractor shall:

5.3.1 TECHNICAL WORKSHOP SUPPORT

The Contractor shall develop and lead a virtual Release-specific Technical Workshop that provides customized information for each LCMS software release. The Contractor shall use the standard video conferencing software currently in use by VA (at this time it is Microsoft Lync). The Contractor shall provide a Technical Workshop Agenda with the topics to be presented. These workshops shall be

developed for a technical audience, providing information of technical significance and include the cumulative deltas between VA's production system, any revised requirements, and the Release. At a minimum the workshop shall include discussing the effects of each Release configuration and modification decision that needs to be made as well as confirming the integrity and accuracy of the current VA LCMS configuration.

Technical Workshops shall be designed to be no more than 40 hours of participant time; length being based on the complexity of the Release. The Contractor shall document the decisions made and action items identified in Workshop Minutes.

Deliverables:

- A. Technical Workshop Agenda
- B. Workshop Minutes

5.3.2 IMPLEMENTATION PLANNING

The Contractor shall develop a detailed Implementation Plan for each Release that shall include a schedule listing all the tasks that must be performed in order to ensure a smooth implementation of the Release. The schedule shall include milestone dates, task durations, and individuals responsible for completing each task. As part of the Implementation Plan, the Contractor shall also prepare a Roll Back Plan for each Release in the event the implementation is not successful.

Deliverable:

- A. Implementation Plan
- B. Roll Back Plan

5.3.3 TEST SUPPORT

In the past, VA has contracted for extensions to the base Kenexa LCMS product to support VA specific requirements and processes. Due to these Extensions, VA requires additional technical support for the Kenexa LCMS application than is available through the standard license maintenance agreement. The Contractor shall provide support related to the extensions to ensure they continue to work as designed.

During the course of VA's User Acceptance Testing (UAT), the Contractor shall be available to respond to questions and concerns by the VA testers about the extensions. During the course of the testing, it may be necessary for the Contractor to modify the extensions to ensure they continue to work as designed after the Release is applied. The Contractor shall deliver the revised extension code to VA staff to apply to the testing environment. The UAT continues until the Contractor has remediated all deficiencies and problems found with the extensions.

At the conclusion of the UAT, the Contractor shall update the Software Design Document (SDD) to match VA's configuration.

Deliverables:

- A. Updated SDD
- B. Revised Extension Code

5.4 LCMS TECHNICAL INTERCHANGE MEETINGS & TECHNICAL SUPPORT

The Contractor shall conduct and administratively support Technical Interchange Meetings (TIMs) at the Contractor's facility or telephonically. During TIMs, the Contractor shall prepare, present, and discuss with VA, specific technical issues relating to LCMS. This may include analysis of new requirements to determine if the LCMS can perform the desired functions "out of the box," or if a new extension may be needed.

All information related to and resulting from the TIMs shall be compiled, summarized, and placed in a TIM Report email. TIMs will be conducted weekly.

The Contractor shall participate as a technical expert during LCMS Community of Practice conference calls anticipated to occur twice a month.

Deliverable:

- A. Technical Interchange Meeting Report Email

5.5 LCMS Authoring Licenses

The VA has tested this product and has previously purchased 280 software LCMS Authoring Licenses. Continued use of this product requires renewal of these licenses. The contractor shall provide renewal of these licenses in support of this contract.

Deliverable:

- A. 280 LCMS Authoring Licenses (280 Authors)

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

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

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are PIV-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), <http://www.ea.oit.va.gov/EAOIT/OneVA/EAETA.asp>, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/docs_design_patterns.asp. The Contractor shall ensure all Contractor delivered applications and systems are compliant with VA Identity Management Policy (VAIQ# 7011145), Continued Implementation of Homeland Security Presidential Directive 12

(VAIQ#7100147), and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document), located at <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>. The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63-2, VA Handbook 6500 Appendix F, "VA System Security Controls", and VA IAM enterprise requirements for both direct and assertion based authentication. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of both Personal Identity Verification (PIV) and Common Access Card (CAC). Assertion authentication at a minimum must include Security Assertion Markup Language (SAML) token authentication and authentication/account binding based on trusted headers. Specific Identity and Access Management PIV requirements are set forth in OMB Memoranda M-04-04 (<http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf>), M-05-24 (<http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf>), M-11-11 (<http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf>), National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, and supporting NIST Special Publications. For applications, software, or hardware that cannot support PIV authentication, a Risk Based Decision must be approved by the Deputy Assistant Secretary for Information Security.

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

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

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 9 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Internet Explorer 11, Office 2013, and Windows 8.1. However, Internet Explorer 11, Office 2013 and Windows 8.1 are not the VA standard yet and are currently not approved for use on the VA Network, but are in-process for future approval by OI&T. Upon the release approval of Internet Explorer 11, Office 2013, and Windows 8.1 individually as the VA standard, Internet Explorer 11, Office 2013, and Windows 8.1 will supersede Internet Explorer 9, Office

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

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

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

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

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

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

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

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

	Position Sensitivity and Background Investigation Requirements		
<u>Task Number</u>	<u>Tier1 / Low / NACI</u>	<u>Tier 2 / Moderate / MBI</u>	<u>Tier 4 / High / BI</u>
5.1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
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"/>

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

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

- a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
- b. The Contractor shall bear the expense of obtaining background investigations.
- c. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the ProPath template. The Contractor Staff Roster shall contain the Contractor’s Full Name, Date of Birth, Place of Birth, individual background investigation level requirement

- (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.
- d. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
 - e. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
 - 1) For a Tier 1/Low Risk designation:
 - a) OF-306
 - b) DVA Memorandum – Electronic Fingerprints
 - 2) For Tier 2/Moderate or Tier 4/High Risk designation:
 - a) OF-306
 - b) VA Form 0710
 - c) DVA Memorandum – Electronic Fingerprints
 - f. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management’s (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
 - g. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a “click to sign” process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via eQIP).
 - h. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.

- i. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or “Closed, No Issues” (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed “Contractor Rules of Behavior.” However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).
- j. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
- k. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.

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: Microsoft (MS) Word 2000/2003/2007/2010, MS Excel 2000/2003/2007/2010, MS PowerPoint 2000/2003/2007/2010, MS Project 2000/2003/2007/2010, MS Access 2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

6.4 PERFORMANCE METRICS

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

Performance Objective	Performance Standard	Acceptable Performance Levels
A. Technical Needs	<ol style="list-style-type: none"> 1. Shows understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Offers quality services/products 	Satisfactory or higher

<p>B. Project Milestones and Schedule</p>	<ol style="list-style-type: none"> 1. Quick response capability 2. Products completed, reviewed, delivered in timely manner 3. Notifies customer in advance of potential problems 	<p>Satisfactory or higher</p>
<p>C. Project Staffing</p>	<ol style="list-style-type: none"> 1. Currency of expertise 2. Personnel possess necessary knowledge, skills and abilities to perform tasks 	<p>Satisfactory or higher</p>
<p>D. Value Added</p>	<ol style="list-style-type: none"> 1. Provided valuable service to Government 2. Services/products delivered were of desired quality 	<p>Satisfactory or higher</p>

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

6.5 FACILITY/RESOURCE PROVISIONS

All procedural guides, reference materials, and program documentation for the project and other Government applications will be provided on an as-needed basis.

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

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

6.6 GOVERNMENT FURNISHED PROPERTY

None

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

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

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

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

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

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

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

A2.0 VA Enterprise Architecture Compliance

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

A2.1. VA Internet and Intranet Standards:

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

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

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

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

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

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

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

- § 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

Offerors shall use the appropriate Section 508 Standards Checklists to ensure conformance with Section 508 Standards. The Standards Checklists along with additional information are available at http://www.section508.va.gov/section508/Standards_Checklist.asp.

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

The Government reserves the right to independently test for 508 Compliance before delivery. The Contractor shall be able to demonstrate 508 Compliance upon delivery.

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.

A4.0 Physical Security & Safety Requirements:

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

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

A5.0 Confidentiality and Non-Disclosure

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

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

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are

- protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA Contracting Officer will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA Contracting Officer for response.
 3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
 4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA Contracting Officer.
 5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
 6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
 7. Contractor must adhere to the following:
 - a. The use of "thumb drives" or any other medium for transport of information is expressly prohibited.
 - b. Controlled access to system and security software and documentation.
 - c. Recording, monitoring, and control of passwords and privileges.
 - d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
 - e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
 - f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
 - g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
 - h. Contractor does not require access to classified data.

8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
9. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

A6.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13514, “Federal Leadership in Environmental, Energy, and Economic Performance,” dated October 5, 2009; Executive Order 13423, “Strengthening Federal Environmental, Energy, and Transportation Management,” dated January 24, 2007; Executive Order 13221, “Energy-Efficient Standby Power Devices,” dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, FEMP designated, low standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

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

1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).
2. Provide/use the purchasing specifications listed for FEMP designated products at www.femp.energy.gov/procurement. The Contractor shall use the low standby power products specified at <http://energy.gov/eere/femp/low-standby-power-products>.
3. Provide/use EPEAT registered products as specified at www.epeat.net. The acquisition of Silver or Gold EPEAT registered products is encouraged over Bronze EPEAT registered products. At a minimum, the Contractor shall acquire EPEAT® Bronze registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified product lists. The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists.

4. The Contractor shall use these products to the maximum extent possible without jeopardizing the intended end use or detracting from the overall quality delivered to the end user.

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

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

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

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

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

B1. GENERAL

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

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 Contracting Officer 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 Contracting Officer 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 Contractor/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 Contracting Officer 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.

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 1600.01, *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 contracting officer 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 contracting officer for response.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or a Memorandum of Understanding-Interconnection Service 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

1. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, *VA Information Security Program*). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6508, *VA Privacy Impact Assessment*.
2. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.
3. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default “program files” directory and silently install and uninstall.
4. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.
5. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.
6. The Contractor/Subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.
7. The Contractor/Subcontractor agrees to:
 - a. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

- i. The Systems of Records (SOR); and
- ii. The design, development, or operation work that the Contractor/Subcontractor is to perform;
 - b. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and
 - c. Include this Privacy Act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR

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

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

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

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

9. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as "Systems"), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hot fixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, based on the severity of the incident.

11. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes based upon the requirements identified within the contract.

12. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the contracting officer and the VA Assistant Secretary for Office of Information and Technology.

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

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must be reviewed and approved by VA prior to implementation.

b. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

c. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization) (C&A) of the Contractor's systems in accordance with VA Handbook 6500.3, *Certification and Accreditation* and/or the VA OCS Certification Program Office. Government-owned (Government facility or Government equipment) Contractor-operated systems, third party or business partner networks require memorandums of understanding and

interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

d. The Contractor/Subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer and the ISO for entry into the VA POA&M management process. The Contractor/Subcontractor must use the VA POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the Government. Contractor/Subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/Subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

e. The Contractor/Subcontractor must conduct an annual self-assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The Government reserves the right to conduct such an assessment using Government personnel or another Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

f. VA prohibits the installation and use of personally-owned or Contractor/Subcontractor owned equipment or software on the VA network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

g. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment

by the Contractor/Subcontractor or any person acting on behalf of the Contractor/Subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the Contractors/Subcontractors that contain VA information must be returned to VA for sanitization or destruction or the Contractor/Subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

h. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

- 1) Vendor must accept the system without the drive;
- 2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or
- 3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.
- 4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;
 - a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and,
 - b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.
 - c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

B6. SECURITY INCIDENT INVESTIGATION

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.

a. 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.

b. 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.

c. 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.

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 Security and Privacy Incidents*, 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.

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.

B.8 SECURITY CONTROLS COMPLIANCE TESTING

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

B.9 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 the VA program official and provided to the contracting officer for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.*]
- b. The Contractor shall provide to the contracting officer and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week 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.

POINTS OF CONTACT:

VA Program Manager:

Name: Timothy E. Sipes
Address: 12656 Lee School Road
Wilton, CA 95693
Voice: (650) 384-3917
Email: timothy.sipes@va.gov

Contracting Officer's Representative:

Name: James Ervin
Address: St. Petersburg OIT Field Office [005OP4G(SP)]
City Center – North Building
100 Second Ave. S., Suite 300
St. Petersburg, FL 33701
Voice: (727) 502-1331
Email: james.ervin@va.gov

SECTION C - CONTRACT CLAUSES

C.1 NASA SEWP V RFQ INTRODUCTORY LANGUAGE

All clauses and provisions from the Federal Acquisition Regulation (FAR), NASA FAR Supplement, and the Goddard Space Flight Center Regulation from the applicable NASA Solutions for Enterprise Wide Procurement (SEWP) V Government-Wide Acquisition Contract (GWAC), and the specific NASA SEWP V contract referenced on the SF1449 in Block 2, are hereby incorporated by reference. The full text of any FAR and NASA SEWP V clauses which are incorporated by reference may be obtained at the following URLs:

FAR: <http://www.acquisition.gov/far/index.html>

NASA SEWP V:

http://www.sewp.nasa.gov/documents/SEWP_V_CLAUSE_LIST.pdf

C.2 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

<http://www.acquisition.gov/far/index.html>

<http://www.va.gov/oal/library/vaar/>

(End of Clause)

<u>FAR Number</u>	<u>Title</u>	<u>Date</u>
52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS	APR 2014
52.204-9	PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL	JAN 2011
52.227-1	AUTHORIZATION AND CONSENT	DEC 2007
52.227-2	NOTICE AND ASSISTANCE REGARDING PATENT AND COPYRIGHT INFRINGEMENT	DEC 2007
52.227-19	COMMERCIAL COMPUTER SOFTWARE LICENSE	DEC 2007

C.3 VAAR 852.203-70 COMMERCIAL ADVERTISING (JAN 2008)

The bidder or offeror agrees that if a contract is awarded to him/her, as a result of this solicitation, he/she will not advertise the award of the contract in his/her commercial advertising in such a manner as to state or imply that the Department of Veterans Affairs endorses a product, project or commercial line of endeavor.

(End of Clause)

C.4 VAAR 852.232-72 ELECTRONIC SUBMISSION OF PAYMENT REQUESTS (NOV 2012)

(a) *Definitions.* As used in this clause—

(1) *Contract financing payment* has the meaning given in FAR 32.001.

(2) *Designated agency office* has the meaning given in 5 CFR 1315.2(m).

(3) *Electronic form* means an automated system transmitting information electronically according to the

Accepted electronic data transmission methods and formats identified in paragraph (c) of this clause. Facsimile, email, and scanned documents are not acceptable electronic forms for submission of payment requests.

(4) *Invoice payment* has the meaning given in FAR 32.001.

(5) *Payment request* means any request for contract financing payment or invoice payment submitted by the contractor under this contract.

(b) *Electronic payment requests.* Except as provided in paragraph (e) of this clause, the contractor shall submit payment requests in electronic form. Purchases paid with a Government-wide commercial purchase card are considered to be an electronic transaction for purposes of this rule, and therefore no additional electronic invoice submission is required.

(c) *Data transmission.* A contractor must ensure that the data transmission method and format are through one of the following:

(1) VA's Electronic Invoice Presentment and Payment System. (See Web site at <http://www.fsc.va.gov/einvoice.asp>.)

(2) Any system that conforms to the X12 electronic data interchange (EDI) formats established by the Accredited Standards Center (ASC) and chartered by the American National Standards Institute (ANSI). The X12 EDI Web site (<http://www.x12.org>) includes additional information on EDI 810 and 811 formats.

(d) *Invoice requirements.* Invoices shall comply with FAR 32.905.

(e) *Exceptions.* If, based on one of the circumstances below, the contracting officer directs that payment requests be made by mail, the contractor shall submit payment requests by mail through the United States Postal Service to the designated agency office. Submission of payment requests by mail may be required for:

(1) Awards made to foreign vendors for work performed outside the United States;

(2) Classified contracts or purchases when electronic submission and processing of payment requests could compromise the safeguarding of classified or privacy information;

(3) Contracts awarded by contracting officers in the conduct of emergency operations, such as responses to national emergencies;

(4) Solicitations or contracts in which the designated agency office is a VA entity other than the VA Financial Services Center in Austin, Texas; or

(5) Solicitations or contracts in which the VA designated agency office does not have electronic invoicing capability as described above.

(End of Clause)

C.5 VAAR 852.237-70 CONTRACTOR RESPONSIBILITIES (APR 1984)

The contractor shall obtain all necessary licenses and/or permits required to perform this work. He/she shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract. He/she shall be responsible for any injury to himself/herself, his/her employees, as well as for any damage to personal or public property that occurs during the performance of this contract that is caused by his/her employees fault or negligence, and shall maintain personal liability and property damage insurance having coverage for a limit as required by the laws of the State of . Further, it is agreed that any negligence of the Government, its officers, agents, servants and employees, shall not be the responsibility of the contractor hereunder with the regard to any claims, loss, damage, injury, and liability resulting there from.

(End of Clause)

C.6 VAAR 852.246-71 INSPECTION (JAN 2008)

Rejected goods will be held subject to contractors order for not more than 15 days, after which the rejected merchandise will be returned to the contractor's address at his/her risk and expense. Expenses incident to the examination and testing of materials or supplies that have been rejected will be charged to the contractor's account.