



Draft Performance Work Statement

**DEPARTMENT OF VETERANS AFFAIRS (VA)
Office of Information & Technology
National Center for Ethics in Health Care**

**Web Based Software Solution for
Signature Informed Consent for Clinical Treatments and Procedures and
Completion of Multiple VA Forms and Support of Software Solution**

DRAFT

**Date: February 6, 2018
Version 0.1**

Contents

1	BACKGROUND	4
2	APPLICABLE DOCUMENTS	5
3	SCOPE OF WORK	7
4	PERFORMANCE DETAILS	8
4.1	PERFORMANCE PERIOD.....	8
4.2	PLACE OF PERFORMANCE.....	8
4.3	TRAVEL	9
5	SPECIFIC TASKS AND DELIVERABLES	9
5.1	CONTRACTOR PROJECT MANAGEMENT.....	9
5.1.1	TECHNICAL KICK-OFF MEETING	10
5.2	SOFTWARE REQUIREMENTS	11
5.2.1	SIGNATURE CAPTURE.....	12
5.2.2	DOCUMENT PROCESSING	12
5.2.3	USER EXPERIENCE.....	13
5.2.4	CLINICAL RESOURCES.....	14
5.2.5	PROGRAM ADMINISTRATION TOOLS	14
5.2.6	INTERFACE TOOLS	15
5.2.7	GRAPHIC REPORT	16
5.2.8	508 COMPLIANCE CERTIFICATION	16
5.3	SOFTWARE MAINTENANCE AND SUPPORT	16
5.4	SOFTWARE DEVELOPMENT	19
5.4.1	WEB-BASED VERSION OF ELECTRONIC INFORMED CONSENT SOFTWARE.....	19
5.5	TRAINING PACKAGES (OPTIONAL TASK).....	20
6	GENERAL REQUIREMENTS	20
6.1	PERFORMANCE METRICS	20
6.2	ENTERPRISE AND IT FRAMEWORK.....	21
6.3	SECURITY AND PRIVACY REQUIREMENTS	23
6.3.1	Position/Task Risk Designation Level(s).....	23
6.3.2	Position Sensitivity and BI Requirements by Task.....	24
6.3.3	Contractor Personnel Security Requirements.....	24
6.4	METHOD AND DISTRIBUTION OF DELIVERABLES	26

6.5	FACILITY/RESOURCE PROVISIONS	26
6.6	GOVERNMENT FURNISHED PROPERTY	27
6.7	CONTINUITY OF SERVICES	27
ADDENDUM A – VA VETERAN FOCUSED INTEGRATION PROCESS (VIP) SOFTWARE REQUIREMENTS		A-1
ADDENDUM B – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED.....		B-1
ADDENDUM C – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE and SCHEDULE OF DELIVERABLES		C-1

1 BACKGROUND

The mission of the Department of Veterans Affairs (VA), Office of Information and Technology (OI&T) is to develop and maintain Information Technology (IT) products and systems that serve our Veterans by supporting the work of the Veterans Health Administration (VHA), Veterans Benefits Administration, and the National Cemetery Administration.

VHA is the largest integrated health care system in the United States, consisting of 150 medical centers and nearly 1,400 community-based outpatient clinics, community living centers, Vet Centers and Domiciliaries. Together, these health care facilities and the more than 53,000 independently-licensed health care practitioners who work within them, provide comprehensive care to more than 8.3 million Veterans each year. VHA personnel practice all medical specialties and provide medical and rehabilitative treatment of all kinds, from acute to long term care to outpatient care.

Within VHA, the National Center for Ethics in Health Care (NCEHC) serves as the authoritative resource for addressing complex ethical issues relating to clinical ethics, organizational ethics, organizational policy, and research ethics. NCEHC works with OI&T to provide technology to empower patients and promote shared decision making through use of a software application that helps clinicians manage the informed consent process electronically.

VHA's NCEHC is the business owner of the requirement for signature informed consent software that assists VA health care professionals in documenting patients' signature and informed consent for over 2,000 treatments/procedures that require signature informed consent. The software also documents Veterans' completion of VA Form 10-0137, "VA Advance Directive and Durable Power of Attorney for Health Care" (Advance Directive). All of these forms require the electronic capture and storage of the patient's and provider's handwritten signature on a specific VA form for storage in the electronic health record with an associated progress note. These signed forms are stored as electronic images in VA's Veterans Health Information Systems and Technology Architecture (VistA) Imaging software system.

VA requires functionality for electronic signature informed consent, patient education documents, and graphic images for all medical specialties, storage in the VA electronic patient health record and single sign on capability through the use of a Personal Identification Verification (PIV) card.

The VA OI&T uses the Veteran-focused Integration Process (VIP) project management process for coordinating development, testing, and deployment of new software functionality requirements. The VIP is a Lean-Agile framework that services the interest of Veterans through the efficient streamlining of activities that occur within the Enterprise. The VIP Guide is located at

<https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>, and provides VA contractors with information on the VIP process.

2 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement (PWS), the contractor shall comply with the following:

1. "Veteran Focused Integration Process Guide 1.0", December 2015, http://www.ea.oit.va.gov/docs/Dec_2016_Release_Docs/VIP_Memo_Guide.pdf
2. POLARIS Release Guide, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4412>
3. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002."
4. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules."
5. FIPS Pub 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013.
6. 10 U.S.C. § 2224, "Defense Information Assurance Program."
7. 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.
8. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
9. 42 U.S.C. § 2000d, "Title VI of the Civil Rights Act of 1964"
10. VA Directive 0710, "Personnel Suitability and Security Program," June 4, 2010, https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=487&FTYPE=2
11. VA Handbook 0710, Personnel Suitability and Security Program, September 10, 2004, <https://www1.va.gov/vapubs/>.
12. VA Directive and Handbook 6102, "Internet/Intranet Services," July 15, 2008.
13. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
14. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," November 28, 2000
15. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
16. 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.
17. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004.
18. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, 2012.

19. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," September 20, 2012.
20. VA Handbook 6500.1, "Electronic Media Sanitization," March 22, 2010.
21. VA Handbook 6500.2, "Management of Data Breaches Involving Sensitive Personal Information (SPI)," January 6, 2012.
22. VA Handbook 6500.3, "Assessment, Authorization, And Continuous Monitoring Of VA Information Systems," February 3, 2014.
23. VA Handbook, 6500.5, "Incorporating Security and Privacy in System Development Lifecycle" March 22, 2010.
24. VA Handbook 6500.6, "Contract Security," March 12, 2010.
25. Technical Reference Model (TRM) (reference at <http://www.va.gov/trm/TRMHomePage.asp>).
26. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008.
27. VHA Directive 6300, Records Management, July 10, 2013.
28. VA Directive 6300, Records and Information Management, February 26, 2009.
29. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010.
30. OMB Memorandum, "Transition to IPv6," September 28, 2010.
31. VA Directive 0735, HSPD-12 Program, February 17, 2011.
32. VA Handbook 0735, HSPD-12 Program, March 20, 2014.
33. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006.
34. OMB Memorandum 05-24, Implementation of HSPD-12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005.
35. 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.
36. OMB Memorandum, Guidance for HSPD-12 Implementation, May 23, 2008.
37. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011.
38. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008.
39. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007.
40. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013.
41. Draft NIST Special Publication 800-157, Guidelines for Derived PIV Credentials, March 2014.
42. NIST Special Publication 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012.
43. Draft National Institute of Standards and Technology Interagency Report

- (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014.
44. VA Memorandum, VAIQ #7100147, Continued Implementation of HSPD-12, April 29, 2011. (Reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>).
 45. 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>).
 46. 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>) .
 47. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, October 1, 2013
 48. OMB Memorandum M-08-05, "Implementation of Trusted Internet Connections (TIC), November 20, 2007
 49. OMB Memorandum M-08-23, Securing the Federal Government's Domain Name System Infrastructure, August 22, 2008
 50. VA Memorandum, VAIQ #7497987, Compliance – Electronic Product Environmental Assessment Tool (EPEAT) – IT Electronic Equipment, August 11, 2014 (reference Document Libraries, EPEAT/Green Purchasing.
 51. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007.
 52. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005.
 53. Executive Order 13514, "Federal Leadership in Environmental, Energy, and Economic Performance," October 5, 2009.
 54. Executive Order 13423, "Strengthening Federal Environmental, Energy, and Transportation Management," January 24, 2007.
 55. Executive Order 13221, "Energy-Efficient Standby Power Devices," August 2, 2001.
 56. VA Directive 0058, "VA Green Purchasing Program," July 19, 2013.
 57. VA Handbook 0058, "VA Green Purchasing Program", July 19, 2013.
 58. VHA Handbook 1907.01 "Health Information Management and Health Records," July 22, 2014.
 59. VA Handbook 1004.01, "Informed Consent for Clinical Treatments and Procedures," August 14, 2009.
 60. VA Handbook 1004.02, "Advance Care Planning and Management of Advance Directives", December 24, 2013.
 61. VA Handbook 1004.05, "iMedConsent™", December 10, 2014.

3 SCOPE OF WORK

The contractor shall provide and maintain a software solution capable of documenting

signature informed consent for treatments and procedures, advance directives, and other VA Forms, for all clinical specialties at each of VHA's 150 medical centers located in all 50 states, Puerto Rico, Guam, and the Philippines.

The contractor shall provide updates to new and existing form content and provide technical maintenance and support for the software.

The contractor shall provide a web-based version of its electronic informed consent software that is compatible with the VA's enterprise architecture. The contractor shall ensure the software has PIV user sign-on capability.

The contractor shall provide computer-based training for administrative functions and use of the software, as set forth in Option 1.

The contractor shall follow an agile methodology and follow the VIP program management process. The contractor shall provide Operations and Maintenance (O&M) support for the software and the features developed as a result of this PWS.

4 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The anticipated period of performance (POP) shall be 12 months from date of award with four (4) 12-month option periods. The POP for the optional task for Training Package development shall not exceed four months from the date the option is exercised. The POP for the optional task to develop a web-based version of the electronic informed consent software shall not exceed 11 months from the date the option is exercised. The total POP of the contract shall not exceed five years.

4.2 PLACE OF PERFORMANCE

Tasks under this PWS shall primarily be performed at the contractor's facilities. Work at the Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO) or the Contracting Officer's Representative (COR).

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 (6) 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

4.3 TRAVEL

The Government encourages the contractor to maximize its use of teleconferencing and video conferencing for meetings.

The Government anticipates travel to perform the tasks associated with the optional task to develop a web-based version of the electronic informed consent software. Travel shall be in accordance with the Federal Travel Regulations and requires advanced concurrence by the COR.

The total estimated number of trips, duration, and attendance is provided below:

PWS	Anticipated Destination	Number of trips	Length of each trip (Days)	Number of Staff traveling per trip
Web-based Tasks	Southwest Continental U.S.	1	3	1
Web-based Tasks	Northwest Continental U.S.	1	3	1
Web-based Tasks	Southeast Continental U.S.	1	3	1
Web-based Tasks	Northeast Continental U.S.	1	3	1

5 SPECIFIC TASKS AND DELIVERABLES

5.1 CONTRACTOR PROJECT MANAGEMENT

The contractor shall designate a contractor Project Manager (PjM) as its main point of contact (POC) between the VA Project Manager (PM) and the contractor's organization. The PjM shall oversee and manage the schedule and all tasks associated with this PWS.

The contractor shall:

1. Provide a staffing assignment worksheet in accordance with section 6.3.3 of this PWS.

2. Maintain a contractor Project Management Plan (PMP) that describes the technical approach, organizational resources, and management controls to be employed to meet the schedule and performance requirements of all deliverables, as defined in this PWS. The PMP shall include a risk management plan and a communication plan.
3. Collaborate with the VA Enterprise Architecture (EA) team and other VA organizations as necessary to develop and maintain deliverables and perform the tasks specified herein.
4. Collaborate with project stakeholders to identify, prioritize, scope, bound, resource, and assess course of actions related to program risks. The contractor shall inform the VA PM of relevant deliberations and contractor recommendations.
5. Work to mitigate and resolve project risks as they are identified.
6. Provide a Monthly Progress Report (MPR). The MPR shall report activities completed in the prior month and activities planned for the next month. The MPR shall include a project status summary, change request status (new, open, and closed since last report), issue/action item status (new, open, and closed since last report), risk items and their disposition.
7. Create meeting minutes for all conference calls and meetings held with the VA PM.
8. The contractor shall notify the VA PM, Contracting Officer's Representative (COR), and CO, in writing, immediately if the contractor is aware of anything that adversely impacts the contractor's performance under this PWS.

Deliverables:

- A. Staffing Assignment Worksheet.
- B. TMS Certificates for IBM Rational Tools Courses
- C. VA Privacy and Information Security Awareness and Rules of Behavior Training Certificate
- D. Signed Contractor Rules of Behavior
- E. VA HIPAA Certificate of Completion
- F. PMP and updates.
- G. MPR.

5.1.1 TECHNICAL KICK-OFF MEETING

The contractor shall hold a technical kick-off meeting within ten (10) days after award, via telephone or in person. The contractor shall present the details of its intended approach, work plan, and project schedule. The contractor shall specify dates and provide all attendees with an electronic copy of the agenda at least five (5) days before the meeting. The contractor shall invite the CO, Contract Specialist, COR, the VA PM and the VA Business Owner. The contractor shall provide meeting minutes to all attendees within three (3) calendar days after the meeting.

Deliverable:

Kick-off meeting agenda and meeting minutes.

5.2 SOFTWARE REQUIREMENTS

The contractor shall provide a web-based version of electronic informed consent software that is in accordance with VHA Handbook 1004.01, "Informed Consent for Clinical Treatments and Procedures," this software shall support documentation of signature informed consent for all treatments and procedures conducted by VHA facilities that require signature informed consent. The software shall electronically capture patient, patient surrogate, practitioner, and witness handwritten signatures as images on documents, with date/time stamps for the handwritten signatures. The software and content libraries shall allow VA professionals to accurately and consistently document signature informed consent for all treatments/procedures requiring signature informed consent, as well as complete multiple VA Forms.

The Contractor shall provide an Enterprise-wide site license for an unlimited number of users. The Government will not pay any additional costs for additional users or sites. The software solution shall provide a real-time interface with VA's VistA and VistA Imaging that interacts with the VistA Text Integration Utility and VistA Imaging Background Processor, using Remote Procedure Calls (RPC). In addition, the software solution shall include a real-time interface with the VA Computerized Patient Record System (CPRS). The VistA interface for transfer of consent form data must be functional at the time of award.

The contractor shall provide software developed to remain in compliance with VHA informed consent policy (Handbook 1004.01 Handbook 1004.05, and VHA Directive 1005) and VHA advance care planning policy (Handbook 1004.02). The contractor shall detail policy compliance by the following:

- The contractor shall provide software that manages patient context/patient selection: Patient selection shall be made by selecting the patient in the associated CPRS and launching the application as an option from within the electronic health record.
- The contractor shall provide software that will include a library of consent forms for all treatments/procedures conducted by VHA for inpatient and outpatient care. The specialties shall include, as a minimum: Anesthesia, Pain Management, Bariatric Medicine, Cardiac Surgery, Cardiology, Dentistry, Dermatology, Emergency Medicine, Gastroenterology, General Surgery, Hematology/Oncology, Interventional Radiology, Mental Health, Nephrology, Neurology, Neurosurgery, Nuclear Medicine, Obstetrics/Gynecology, Ophthalmology, Orthopedic Surgery, Otolaryngology, Physical Medicine/Rehabilitation, Plastic / Reconstructive Surgery, Podiatry, Pulmonary Medicine, Radiation Oncology, Radiology (Diagnostic), Rheumatology, Thoracic Surgery, Urology, and Vascular Surgery.
- The contractor shall provide software with a document library that will provide consent forms in English and Spanish, written to a 6th - 8th grade reading level.

- The contractor shall provide software with consent forms that include a description of the specific treatment/procedure, its risks, benefits, alternatives, and a patient and practitioner attestation statement. The treatment/procedure specific information shall populate onto a standardized electronic presentation of a VA form and include demographic data needed to complete the form (e.g., VA Form 10-0431a, "Consent for Clinical Treatment/Procedure", VA Form 10-0431b, "Consent for Transfusion of Blood Products"; VA Form 10-0431c, "Consent for Long-Term Opioid Therapy for Pain").
- The contractor shall provide processes that document patient decision-making capacity as part of consent form completion. Users are required to select whether the patient has decision-making capacity (DMC). Depending on the answer, the program shall offer options. If the patient has DMC, the consent documentation process begins. If the patient lacks DMC, the user is queried on the reason for this determination (e.g., clinical evaluation used to make determination, patient is a minor, or patient has been ruled incompetent by a court). An option for surrogate designation/documentation shall apply to all consent forms for treatments and procedures, and apply to non-consent forms only on a case-by-case basis. If the patient lacks DMC, the software shall allow documentation of the patient's surrogate by name and relationship. Should the surrogate be physically available, signature fields and attestation statements shall allow for documenting that the signature was obtained from the surrogate. Should the surrogate not be physically available, the software shall allow for documenting the informed consent process being conducted telephonically between the provider and the surrogate. Documentation that the surrogate's consent was obtained telephonically shall require signature of the provider obtaining informed consent. The software shall require the provider to annotate whether the required witness is co-located with the provider and can sign the form, as well as document witnessing the conversation in a progress note within the electronic health record. The witness shall be able to sign the document if co-located with the provider.

5.2.1 SIGNATURE CAPTURE

The contractor shall provide software that incorporates processes to capture full and partial signatures (asynchronous consent/signatures), as allowed for by VA policy. The software shall fully support signature-capture devices currently in use by VA. The application shall have the ability to print consent forms and save those documents to a patient's record within VistA Imaging as an Adobe Postscript Data Format (PDF) image, linked to a progress note in VistA CPRS.

5.2.2 DOCUMENT PROCESSING

The contractor shall provide software that has the ability to process documents and populate them into the patient's individual electronic health record as an image with an

associated progress note, though individual documents may be designated by administrators for image storage only, with no progress note associated. Population of these images into VistA Imaging shall include associated document data to allow for user functionality available within the associated system (e.g., image indexing within VA's VistA Imaging, designating saving of the image without an associated progress note, watermarks on partially signed and deleted forms). The software shall have the ability to automatically populate a locally customizable, associated progress note into the electronic health record. The ability to require a progress note for a document can be changed at the local level for local forms and at the local or national level for national forms. The automatically populated progress note shall not require signature by the user, but shall be an administrative note pointing to the existence of the associated image in the imaging system.

Documents shall have an editable interface to allow for defining the electronic processes associated with each document, including: which progress note title the progress note will be given; an option for building business rules establishing logic for activating or inactivating wizard panels in the document's wizard; which wizard shall be associated with the document; setting/editing keywords for document searching; identifying which "category/specialty" shall be available in within the document library; providing reminder screen text; selecting whether the document shall have an associated progress note; and whether the image generated can be stored.

5.2.3 USER EXPERIENCE

The contractor shall provide software with the ability to include the following ease of use features. The application shall be fully Section 508 compliant in accordance with PWS section 5.2.8 and Addendum B. Documents provided for use in the software shall provide users with a selectable, dual English/Spanish language documentation and presentation capability. "Help" support shall be provided using the Microsoft (MS) Windows standard "Help" dropdown. Help shall include an administrator's guide, which shall provide examples of all administrative functions by topic.

The contractor shall provide software with the ability for administrators to build "packages" of documents to ease access (e.g., build a package of documents associated with "Cardiac Catheterization", including consent forms, education documents, and discharge instructions).

The contractor shall provide software with the ability for users to create and maintain a "Favorites" list. Users shall have the ability to have any documents they use be automatically added to their "Favorites" and an option to manually add documents.

The contractor shall provide software with the ability to generate documents for completing informed consent and non-consent forms via a Browser User Interface (BUI), compatible with VA standardized web browsers. The software shall provide users the option to view and select available documents within the library based upon a specialty hierarchy (with options for consent documents, education documents, images,

patient instructions, discharge instructions, and locally customizable specialties and categories). When generating a consent or administrative form, users shall be presented with options that allow for patient verification; automatic selection (or fill-in) of the provider completing the form; selection of providers who are expected to participate in the procedure, surrogate selection options and "reminder screens." When generating a consent form, users shall be presented with an option that allows for documentation and editing of patient's decision-making capacity, reason for treatment/procedure, description of the treatment/procedure, anatomical location, anesthesia/moderate sedation, consent to use of blood products (including patient's reasons for declining if appropriate), benefits, risks, alternatives, facility-specific field for treatments/procedures, and comments. The software shall provide users the option to select one to many procedures to generate a single consent form.

The contractor shall provide software with the capability within each consent document for users to bypass text that usually does not change (e.g., description of procedure, risks, and benefits) and an option to present all consent information to the user. The final document shall be editable by jumping back into any the document development flow and editing sections of the form prior to signature. The software shall have the ability to "hold" a patient-specific document for a specified period with either no signatures or partial signatures. End users shall be able to complete documents held temporarily for signature.

5.2.4 CLINICAL RESOURCES

The contractor shall provide software that incorporates a library of graphic anatomical images, procedure images, and medical system images that can be associated with a specific patient, annotated using graphic drawing tools, and stored in the patient's electronic health record using the software interface.

The contractor shall provide software that incorporates a library of patient educational documents to support instruction/training for the majority of the treatments/procedures provided within VA. The educational document library shall have the ability to add locally developed educational documents and associate them with consent forms, as well as be able to document a patient's comprehension of the education document in accordance with Joint Commission requirements. Forms shall have the ability to be saved to the patient specific record with or without an associated progress note as set nationally or locally. The software shall have the ability to identify, view, and save education documents related/associated with specific procedure or treatment consent forms (e.g., when selecting a consent form for a procedure, the user shall be provided with a list of educational documents associated with that procedure).

5.2.5 PROGRAM ADMINISTRATION TOOLS

The contractor shall provide software with the ability to: create and maintain a "Favorites" list of documents for individual users; save documents into alternative, compiled formats, that include the verbiage from the document's standardized text

(e.g., MS Word, Excel, .pdf); lock documents for editing at the local level or partially lock them, as determined by policy (e.g., national consent forms currently do not allow for local edit of the description of the treatment/procedure, risks, benefits, alternatives, but do allow for editing a field for "facility-specific treatment preferences" and "Additional Comments"); copy and rename documents. The software shall allow for the local administrators to build local consent and administrative documents with all associated fields available in contractor-provided forms (local administrators as well as higher-level administrators). Locally developed forms shall only be available at local sites, while nationally developed forms shall be built and maintained by the contractor. The software shall allow for the import/export of locally developed forms for sharing with other sites. The software shall provide users and administrators with the capability to submit on-line content requests to the contractor. VA software administrators shall be able maintain the software application as defined in VHA Handbook 1004.05. VA Administrative users shall also have the ability to create, edit, and remove documents within the software library.

The software shall provide VA Administrators the ability to identify which progress note title shall be associated with each document saved into the local electronic health record, using current processes for populating notes into the patient record (e.g., VA uses the VistA Text Integration Utility with specific Internal File Number (IFN) numbers to designate progress note titles). The software shall provide VA Administrators the ability to prepopulate document header data with locally customizable headers and the ability to remove or add documents from/to the view of users (nationally/locally as appropriate, based upon defined administrative roles).

The software shall provide the capability to generate a coordinated quarterly (Federal fiscal year) data collection report "pulled" from all facility servers running the software application, deployed in VA, for use by the VA COR and the VA PM. Quarterly software usage reports shall provide the following detail: consent forms saved by facility and specialty; locally created document activity by facility and document title; consent forms saved by facility; activity total and percent change from previous quarter (include past quarters for trending purposes); and non-consent forms printed (include past quarters for trending purposes). The software shall provide VA administrators the ability to generate local reports with and without Personally Identifiable Information (PII) and Protected Health Information (PHI), down to the document level, including: document usage; library content; use of specific features (e.g., surrogate consent by telephone); documents on hold for signature; note number (associated with documents being processed into the electronic health record) and content update data; and the ability to run specific reports based upon a user's and/or administrator's defined role and level of responsibility.

5.2.6 INTERFACE TOOLS

The contractor shall use remote procedure calls (RPC), for the interface between VistA Imaging, VistA, CPRS and the contractor's software solution. The contractor shall provide users a PIV sign on capability that is compatible with the VA system, no later

than 4 months after contract award.

5.2.7 GRAPHIC REPORT

The contractor shall provide a graphic report with screenshots of all wizard panels/applets, updates, and versioning of the software for concurrence by the OI&T PM, VA Business Owner, and COR.

5.2.8 508 COMPLIANCE CERTIFICATION

The contractor shall ensure the software is VA Section 508 compliant. The contractor shall coordinate and complete VA 508 compliance certification in accordance with Addendum B.

Deliverables:

- A. Web-based Signature Informed Consent Compliant Software.
- B. PIV compliant sign-on software
- C. Quarterly Update Usage Reports.
- D. Quarterly Consent Form Updates.
- E. Graphic Report.
- F. 508 Compliance Certification

5.3 SOFTWARE MAINTENANCE AND SUPPORT

The contractor shall provide 24x7x365/366 software maintenance and technical support for the software solution.

The contractor shall provide software maintenance and technical support services, including quarterly updates, enhancements, and corrections to the software, all of which are customarily provided by the contractor to its customers so as to cause the software to perform according to its specifications, documentation, or demonstrated claims. Calls or email requests for support from VA staff shall be returned within two hours.

The contractor shall provide quarterly application updates and releases that include corrections to reported defects, application updates, and associated services, and:

1. Maintain rigorous quality assurance effort, including Alpha testing on VA-specific system configurations and Beta testing at selected VA locations prior to general release.
2. Provide high-quality technical and end-user documentation for each program release.

The contractor shall provide telephone customer service and technical support with respect to the software each business day between the hours of 8:00 am and 6:00 pm Eastern Time.

After hours support shall be provided via after-hours phone service or automatic forwarding to on-call personnel. All after hour calls shall be addressed within two hours of initial contact. In addition, the contractor shall provide web-based technical support 24 hours per day, seven (7) days per week.

Error Corrections: The contractor shall correct all errors reported to the contractor by VA. Error corrections shall be made available via download or delivered via some other media. If the contractor is unable to correct an error remotely, the contractor shall perform on-site support in an attempt to correct the error. The contractor shall provide a history of error correction services and/or operations rendered to VA. The VA will classify the severity level of documented errors as follows:

SEVERITY 1: System inoperable due to a software malfunction. The contractor shall respond to any error that the parties mutually agree has a severity level of one within two hours. Every effort will be made to resolve such errors within twenty-four (24) hours after VA provides the contractor with written notice thereof.

SEVERITY 2: Data files inaccurate or inaccessible, or an error that substantially interferes with VA use of the software due to a software malfunction. The contractor shall respond to any error that the parties mutually agree has a severity level of two within four hours. Every effort will be made to resolve such errors within twenty-four (24) hours after VA provides the contractor with written notice thereof.

SEVERITY 3: Output inaccurate or inaccessible due to a software malfunction. The contractor shall attempt to correct any error that the parties mutually agree has a severity level of three within ten (10) days after VA provides the contractor with written notice of such error.

SEVERITY 4: Informational or minimal impact due to a software malfunction. The contractor shall attempt to correct any error that the parties mutually agree has a severity level of four, within thirty (30) days after VA provides the contractor with written notice of such error.

The contractor shall update the content library for English and Spanish documents on a quarterly basis, if approved content is available from the VA Office of Patient Care Services (VA PCS).

The contractor shall provide regular content library updates that include new and revised clinical procedures, patient education documents, and updated medical images and drug monographs which have been authorized by the VA PCS. The contractor shall add NCEHC approved, VA-specific administrative forms to the standard library at no additional cost to the Government, unless the proposed document requires one or more of the following:

1. Document level security (per document in the ACL)

2. New CPRS data interface
3. Programmable coding changes

The contractor shall maintain the content to comprehensively cover all of the treatments and procedures performed in VA, providing new clinical content as requested by VA PCS. The contractor shall ensure that all newly-developed content is submitted to VA-designated subject matter experts for review and approval before released to the field, as described below. Substantive changes to content that is already in use in VA shall be forwarded to VA PCS for review before release to the content library.

The contractor shall redirect any requests for new content, specialties, changes in content, or changes in business processes made by VA Medical Centers and VA staff to a VA centralized shared mailbox to be set up and monitored by VA PCS. Any links within the software to allow for submission of change suggestions from the field shall be directed to this mailbox. VA PCS will review, coordinate, and forward approved development/change requests to the contractor. Unless otherwise agreed to by VA PCS in advance, the contractor shall deliver the draft electronic informed consent software form for new or updated content within 90 days to VA PCS for review and approval before release to the field. The contractor shall reply back to the email received from VA PCS which should contain:

1. Specific origin of the request and date of request
2. VA Subject Matter Expert identified in original request

The contractor shall add the following text: "Changes made as submitted below." If for any reason the changes vary from what VA PCS requested, an explanation of the changes shall be provided in the email. VA PCS will review and a final determination will be made based upon the current procedure.

The contractor shall not automatically submit existing consent forms for review based upon any time schedule. If the contractor makes revisions to existing informed consent forms based upon an update of current evidence-based information related to any identified procedure, the contractor shall query VA PCS on the desire of VA PCS to make the suggested change. This query shall be accompanied by the evidence-based literature that supports the suggested change and the suggested change language (not the full revised consent). VA PCS will respond to the request via email communication.

New consent forms for procedures or tests, content, specialties, changes in content, or changes in business processes developed independently by the contractor (i.e., absent a request from VA) shall be forwarded to VA PCS for determination of whether the consent form shall be released in VA. When forwarding, the contractor shall clearly state that this is being proposed outside of the VA request process and provide current evidence-based information to support the need for the new content. VA PCS will make the determination to add or reject the proposed content.

The contractor shall deliver support call logs, listing facilities requesting support, issue status, and issue resolution summaries.

Deliverable:

Quarterly Support Call Logs

5.4 SOFTWARE DEVELOPMENT

5.4.1 WEB-BASED VERSION OF ELECTRONIC INFORMED CONSENT SOFTWARE

The contractor shall develop and deploy a web- based version of their electronic informed consent software to all VA facilities currently using another electronic informed consent software version/model. All capabilities listed in 5.2-5.3 shall be included in the web-based version of their electronic informed consent software. .

The contractor shall follow VIP outlined below to coordinate software development, testing, acceptance, installation and implementation for all sites currently using another electronic informed consent software version.

The contractor shall ensure that web-based software developed allows for patient identity management within the VA firewall.

The contractor shall ensure that patient identity management processes used by the software work within the VA architecture.

The contractor shall ensure the software is VA Section 508 compliant 60 days after award. The contractor shall coordinate and complete VA 508 compliance certification in accordance with Addendum B.

The contractor shall conduct a kick-off meeting within 15 days of initiation of this option.

The contractor shall comply with the Veteran focused Integration Process (VIP) for project management and coordination with the VA as provided in Addendum A.

Deliverables:

- A. Product Configuration Management Plan
- B. Version Description Document
- C. VA Compatible version of electronic informed consent Web-Based COTS Software.
- D. VA 508 Compliance Certification.
- E. Test Strategy Data input into Rational
- F. Test Plan and Test Execution Data input into Rational
- G. Requirements Traceability Matrix (RTM) in Rational
- H. Production Operations Manual (POM) and/or Technical Manual
- I. Deployment and Installation Guide
- J. User Manual

5.5 TRAINING PACKAGES (OPTIONAL TASK)

The contractor shall provide two software application training modules to support development of the web-based version of their electronic informed consent software. One training module shall be for software application users and the other shall be for software application administrators. The contractor shall provide a detailed plan for the design and functionality of the education modules. Draft plans and storyboards shall be presented to the VA COR and Business Owner for review and feedback. The contractor shall provide a script and screen shot mock ups to obtain approval of the content of the training modules from the VA COR and Business Owner. The contractor shall incorporate all COR-directed feedback on the prototype modules into the final training modules. The training shall be developed for and deployed on the VA Talent Management System (TMS). The training shall include elements needed for obtaining "Continuing Medical Education" (CME) credit. Each module shall include graphics and screenshots taken from the existing, approved software. To ensure complete functionality within the VA TMS environment, the contractor shall work with VA staff as needed to ensure the course navigates, passes data to and from the TMS correctly, and displays correctly to users of the course. Each module shall include at least ten (10) evaluation questions. The training modules shall meet 508 certification criteria.

Deliverables:

- A. VA Training module scripts and training module screen shot mock ups.
- B. VA Users Training Module on TMS.
- C. VA Administrator Training Module on TMS.

6 GENERAL REQUIREMENTS

6.1 PERFORMANCE METRICS

The table below defines the Performance Metrics associated with this effort.

Performance Objective	Performance Standard	Acceptable Performance Levels
Technical Needs	1. Shows understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements a. Rational inputs are timely, complete and accurate 4. Offers quality services/products	Satisfactory or higher

Project Milestones and Schedule	1. Quick response capability 2. Products completed, reviewed, delivered in timely manner a. POLARIS inputs are timely, complete, and accurate 3. Notifies customer in advance of potential problems	Satisfactory or higher
Project Staffing	1. Currency of expertise 2. Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
Value Added	1. Provided valuable service to Government 2. Services/products delivered were of desired quality	Satisfactory or higher

The Government will use 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 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. The COR will determine if the performance of the contractor is below a metric standard and deem it unacceptable. The COR will then notify the CO.

6.2 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 EA that establishes a common vocabulary and structure for describing the IT 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 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 11 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall

also be compatible with Office 2013 and/or Office 365, and Windows 8.1 and/or 10. However, Office 2013 and 365 and/or Windows 8.1 and/or Windows 10 are not the VA standard yet and are currently not approved for use on the VA Network, but are in-process for future approval by OI&T. Upon the release approval of Office 2013 and/or 365, and Windows 8.1 and/or 10 individually as the VA standard, Office 2013 and/or 365, and Windows 8.1 and/or 10 will supersede Office 2010, and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be delivered as a signed .Microsoft 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 contractor 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 VIP software approval system 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, the VIP software approval system 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 VIP, the OI&T-wide VIP process management tool that assists in the execution of an IT project. VIP is used to build schedules to meet project requirements, regardless of the development methodology employed.

6.3 SECURITY AND PRIVACY REQUIREMENTS

6.3.1 Position/Task Risk Designation Level(s)

Position Sensitivity	Background Investigation (BI) (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 the Office of Personnel Management (OPM) and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the Department of Defense (DOD) Defense Central Investigations Index (DCII), Federal Bureau of Investigation (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

Moderate / Tier 2	Tier 2 / Moderate BI (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 SII, DOD DCII, FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree.
High / Tier 4	Tier 4 / BI A Tier 4/BI is conducted by OPM and covers a 10-year period. It consists of a review of NAC records [OPM SII, DOD 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 BI commensurate with the required level of access for the following tasks within the PWS are:

6.3.2 Position Sensitivity and BI Requirements by Task

Task Number	Tier 1 Low / NACI	Tier 2 Moderate / MBI	Tier 4 High / BI
5.1	X		
5.2	X		
5.3	X		
5.4	X		

The tasks identified above and the resulting position sensitivity and BI requirements identify the BI requirements for contractor individuals, based upon the tasks the particular contractor individual will be working. The submitted contractor staffing assignment worksheet shall indicate the required BI level for each contractor individual, based upon the tasks the contractor individual will be working in accordance with the contractor's submitted proposal.

6.3.3 Contractor Personnel Security Requirements

1. The contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate BI, and are able to read, write, speak, and understand the English language.
2. The contractor shall bear the expense of obtaining BIs.
3. Within three business days after award, the contractor shall provide a staffing assignment worksheet of contractor and subcontractor employees to the COR to begin their BIs in accordance with the ProPath template. The contractor staffing assignment worksheet shall contain the contractor individual's full name, date of birth, place of birth, individual BI level requirement, etc. The contractor shall

submit full Social Security Numbers under separate cover to the COR. The contractor staffing assignment worksheet shall be updated and provided to VA within one day of any changes in employee status, training certification completion status, BI level status, additions/removal of employees, etc. throughout the POP. The contractor staffing assignment worksheet 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 staffing assignment worksheet 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.

4. The contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
5. The contractor shall ensure the following required forms are submitted to the COR within five days after contract award:
 - a. Optional Form 306
 - b. Self-Certification of Continuous Service
 - c. VA Form 0710
 - d. Completed Security and Investigations Center (SIC) Fingerprint Request Form
6. The contractor personnel shall submit all required information related to their BIs (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the OPM Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
 - a. 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 three business days that documents were signed via eQIP).
 - b. 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.
 - c. A contractor may be granted unescorted access to VA facilities and/or access to VA IT resources (network and/or protected data) with a favorably adjudicated special agreement check (SAC), 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 OPM.
 - d. The contractor, when notified of an unfavorably adjudicated BI on a contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.

- e. 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.
- f. 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.

6.4 METHOD AND DISTRIBUTION OF DELIVERABLES

The contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include:

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

6.5 FACILITY/RESOURCE PROVISIONS

The Government will not provide laptop computer, office space, or telephone service in service to this contract.

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

VA will provide access to VA specific systems/network as required for execution of the task via remote access technology (e.g. Citrix Access Gateway (CAG), site-to-site VPN, or VA Remote Access Security Compliance Update Environment (RESCUE)). This remote access will provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, VIP, Primavera, and Remedy, including appropriate seat management and user licenses. The contractor shall use 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 (SSPs) and Authority to Operate (ATOs) for all systems/LANs 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 B – Additional VA requirements, consolidated and ADDENDUM C - VA information and information system security/privacy language.

6.6 GOVERNMENT FURNISHED PROPERTY

The Government will provide access to VA's IBM Rational Collaborative Application Lifecycle Management (CALM) Toolset (hereafter referred to as Rational) to provide a single Agile project/product application lifecycle management toolset to track execution details after contractors complete the training as required in Section 5.1.3. In order to access VA's IBM Rational, the contractor will require VA access. If the mandated toolset changes throughout the period of performance of this contract then the Government will provide access to the new toolset.

GFE is not provided for this work. Laptops, desktops, and servers will not be provided to contractor. Testing environments (hardware, software, or physical space for equipment) for contractor use will not be provided.

6.7 CONTINUITY OF SERVICES

The Contractor recognizes that the services under this contract are vital to the Government and must be continued without interruption and that, upon contract expiration, a successor, either the Government or another contractor, may continue them. The Contractor agrees to (1) furnish phase-in training and (2) exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor.

The Contractor shall, upon the Contracting Officer's written notice, (1) furnish phase-in, phase-out services for up to 90 days after this contract expires and (2) negotiate in good faith a plan with a successor to determine the nature and extent of phase-in, phase-out services required. The plan shall specify a training program and a date for transferring responsibilities for each division of work described in the plan, and shall be subject to the Contracting Officer's approval. The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services called for by this contract are maintained at the required level of proficiency.

The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this contract. The Contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are

agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

The Contractor shall be reimbursed for all reasonable phase-in, phase-out costs (i.e., costs incurred within the agreed period after contract expiration that result from phase-in, phase-out operations) and a fee (profit) not to exceed a pro rata portion of the fee (profit) under this contract.

Addendum A

ADDENDUM A – VA VETERAN FOCUSED INTEGRATION PROCESS (VIP) SOFTWARE REQUIREMENTS

A1.0 VIP Mandatory

Agile project management is evolutionary (iterative & incremental) which regularly produces high quality results in a cost effective, timely, and highly collaborative manner via VIP's value driven lifecycle. This requires open lines of communication among all participants contributing to a project/program/portfolio that include multiple consumers within the contracts and with other VA offices/activities.

VIP describes a schedule of incremental deliveries of useable capabilities every three (3) months or less.

Backlog grooming and prioritization are continued throughout the product life cycle and shall be managed throughout the period of performance. Based on the scope of work established in the backlog, development builds shall be three (3) months or less. The contractor shall develop and deliver a build plan in collaboration with the project team prior to beginning the build. The build plan is the scope of work which will be completed in the agreed upon build timeframe. Each build ends with a new release or push to production. The contractor shall follow the standard development cycle as outlined below in Section 5.3 and all subparagraphs – plan, develop, test, release, performance monitoring and warranty for all builds.

A build will consist of a series of sprints (typically 1-4 weeks duration). The contractor shall provide a sprint plan prior to the beginning each sprint which defines the work to be completed during the sprint. Once the sprint plan is approved by the Government, the Government will establish when the sprint is complete.

The foundational structure for VA agile development and project management can be found in the VIP Guide. For delivery of all project artifacts, the contractor shall use Rational for managing project execution details and for the management and storage of artifacts using approved VIP and/or EPMO website templates.

A2.0 REPORTING REQUIREMENTS

The contractor shall use the VA's implementation of the Rational Toolset to provide a single Agile project/product lifecycle management tool to track execution details. The Rational Project/Product Data and Artifact Repository will be used to provide a single authoritative project and product data and artifact repository. All OI&T project data and artifacts will be required to be managed in this data and artifact repository daily. All checked out artifacts shall be checked back in daily and any data updated daily. Rational synchronizes all changed information immediately for all team members to access work proficiently without the concern of working on aged information.

The contractor shall use VA Rational tools in accordance with the VA Rational Tools Guide to:

Addendum A

1. Input and manage scheduled project/product sprints and backlog
2. Input and manage project/product agile requirements
3. Input and manage project/product risks and issues
4. Input and manage project/product configurations and changes
5. Input and manage project/product test plans and execution
6. Input and manage project/product planning and engineering documentation
7. Input and manage linkages to correlate requirements to change orders to configurable items to risks, impediments, and issues to test cases and test results to show full traceability.

The contractor shall show all Agile requirements, changes, tests performed and test results in Rational to show evidence of code coverage and test coverage of all the requirements specified. This expectation will allow VA to have high confidence in a fully documented, as evidenced by data in the tools, requirements traceability matrix

A3.0 RATIONAL TOOLS TRAINING

The contractor shall complete all of the following VA TMS training courses:

1. TMS ID 3878248 - IBM Rational Team Concert - Agile Sprint, Configuration/Change Management Level 1
2. TMS ID 3878249 - IBM Rational Team Concert - Agile Sprint, Configuration /Change Management Level 2
3. TMS ID 3878250 - IBM Rational DOORS Next Generation - Requirements Management Level 1
4. TMS ID 3897036 - IBM Rational DOORS Next Generation - Requirements Management Level 2
5. TMS ID 3897034 - IBM Rational Quality Manager - Quality Management Level 1
6. TMS ID 3897035 - IBM Rational Quality Manager - Quality Management Level 2

Contractors who have completed these VA training courses within the past 24 months and have furnished certificates will not be required to re-take the training courses.

A4.0 PRIVACY & HIPAA TRAINING

The contractor shall submit TMS training certificates of completion for VA Privacy and Information Security Awareness and Rules of Behavior and Health Insurance Portability and Accountability Act (HIPAA) training, and provide signed copies of the contractor Rules of Behavior in accordance with Section 9, Training, from Appendix C of the VA Handbook 6500.6, "Contract Security."

A5.0 CONFIGURATION MANAGEMENT:

The contractor shall:

- A. Identify the standard and unique aspects of configuration management to be performed for each project by establishing a Product Configuration Management Plan which meets EPMD Website CM plan requirements. The contractor shall reflect all CM required activities and standards in each project-level CM plan while

Addendum A

determining the unique aspects of the project which require individualized procedures.

- B. Deliver a recommended list of configuration items to be placed under configuration and change control. The contractor shall identify types of configuration items pertaining to each product to be placed under configuration management. Based on EPMO requirements, and the unique needs or nature of each project, the contractor shall determine the components within each project that must be under configuration control.
- C. Use Rational Team Concert as the VA approved tool and repository for all software source code and electronic artifact configuration and version management. The contractor shall use IBM Rational Team Concert tool to manage change, activity, issue, action, risk, and other project data as prescribed by VA standards and processes. If assigned a project using tools that are being deprecated, the contractor shall assist the VA Tools Team in migrating projects using other Change and/or Configuration Management tools to the IBM Rational Team Concert tool.
- D. Ensure that all project software and non-software artifacts are versioned correctly according to VA standards and follow a build/release promotion versioning approach which identifies all major, minor, and update changes to the components.
- E. Create Project and Product Artifacts baselined and versioned in the CM repository in order to allow the tool to show active and past histories of the check-ins and check-outs of all software components, data, and software project engineering documents. Maintain all baselines of software, software builds, and electronic artifacts in the repository, labeling updates and versions according to CM procedures.
- F. Develop, verify and submit with all project build deliveries, a Version Description Document that conforms to EPMO Website standard templates and addresses the manifest of the contents of all software builds created for project releases outside the development environment.
- G. Establish and maintain status reporting on change and configuration management activity, and ensure Rational Team Concert data records and artifacts are filed and updated daily.

A6.0 PLANNING

A6.1 AGILE REQUIREMENTS ELABORATION

The contractor shall complete an initial backlog grooming session with the VA team to properly understand and elaborate business Agile requirements. The outcome of this session shall be a complete review of, and agreement to, the initial user stories, including user stories added as a result of backlog grooming by decomposing epics into stakeholder needs, business requirements, business rules, requirements visualizations and user story elaborations.

Addendum A

The contractor shall:

1. Ensure all epics, including Standard Epics as defined in Section 5.5, are included and executed as appropriate within the overall agile backlog grooming effort.
2. Populate the backlog during an initial planning session identifying all features the team considers relevant to building the product. The backlog serves as the primary source for all program requirements and user stories, and the team shall prioritize the contents.
3. Establish initial Unit of measurement (e.g. Story Points) as the estimated relative complexity of user stories.
4. Facilitate any stakeholder briefings, meetings and/or elicitation sessions.
5. Execute requirements reviews with stakeholders and record results of reviews using Rational DOORS Next Generation, updating requirements data as a result of the reviews.
6. Identify the development and test environment access that is needed 30 days prior to development start.
7. All Epics, stakeholder needs, visualizations, stories, and other sources of requirements information for functional and non-functional requirements are Input and maintained in Rational. All requirements data is under change control and is fully linked to work items that show traceability to design changes, configurable items, test cases and test results.

Any attributes that may be identified as new requirements (outside the scope of the Epics as defined in Section 5.5 of this TO) during the backlog grooming sessions may not be incorporated into the Backlog without requesting a formal contract modification from the Contracting Officer (CO) prior to any execution of effort. If the result of the backlog grooming session(s) determines that there are additional requirements that are out of scope, the contractor shall notify the CO.

A6.2 BUILD AND DEVELOPMENT

The contractor shall continuously support the iterative build and development methodology described within Section 5.3 in order to complete all epics and user stories identified in the backlog.

A6.3 BUILD PLANNING

The contractor shall develop a Build Plan prior to the start of each build. Each build shall be no longer than 3 months in duration and shall be made up of individual sprints. Each build will be fully tested by end users and will end in a new release candidate. The contractor shall maintain the program/project backlog, continuously, for each build, in every release and throughout the life of the period of performance within Rational Team Concert. All activity scheduled in each build and backlogs will be captured and have status showing all work items, changes, impediments, and retrospectives. All data and artifacts in Team Concert shall be fully linked to requirements data and test data.

Build planning shall consist of the following:

Addendum A

1. Teams will review, elaborate, and prioritize the backlog. This backlog grooming will occur continuously throughout the build to ensure the customer's highest priorities are being met.
2. Backlog grooming and Build Planning sessions, facilitated by the contractor, that outline the intent of the build, and are not a formal commitment. The contractor shall update the resulting Build Plan within Rational Team Concert.
3. Identification of the epics and user stories to be completed within the build, the agreement of acceptance criteria of the build, and readiness to begin build.
4. Identification of field sites, test environments, acceptance criteria, and ATO requirements.
5. Coordinate and validate MOU's and SLA's for partner dependencies that specifically highlight the commitment of partners to associated release.

A6.4 SPRINT PLANNING

Once the build plan is completed and accepted, the contractor will initiate Sprint Planning for the first Sprint of the build. All activity scheduled in each sprint and backlog will be captured and have status showing all work items, changes, impediments, and retrospectives. All data and artifacts in Rational Team Concert shall be fully linked to requirements data and test data.

The contractor shall:

1. Initiate and participate in a sprint planning meeting, at the beginning of each sprint. The contractor shall update the sprint plan in Rational Team Concert at the conclusion of the Sprint Planning.
2. Support, coordinate and provide input for the sprint acceptance criteria in Rational Team Concert. The Sprint acceptance criteria shall be coordinated and approved for every sprint.

A6.5 SPRINT EXECUTION

All activity executed in each sprint and backlog will be captured and have status showing all work items, changes, risks, issues, impediments, and retrospectives. All data and artifacts in Rational Team Concert shall be fully linked to requirements data and test data. All project artifacts and source code will be under change and configuration management as specified by the COR using Rational.

The contractor shall:

1. Provide a certified Scrum Master to provide the following functions included, but not limited to: facilitate all ceremonies, ensure Rational is updated daily, enforce scrum framework, track and assist with removing impediments.
2. Develop the features and capabilities as work items in Rational Team Concert that were established in the Sprint Plan.
3. Complete sprint development including disciplined testing (unit, functional, regression) and reviews as a continuous process, to avoid finding issues at the end of sprint development.

Addendum A

4. Initiate and conduct daily scrums (typically 15 minutes) to show the team progress, impediments and daily plans.
5. Update Rational daily, to include progress on tasks during sprints, blockers and dependencies.
6. Coordinate and support demonstration of the sprint activities with the project team and Users at the end of each sprint. This is termed a Sprint Review and will result in Customer Acceptance of the Sprint.
7. Develop and deliver automated build and automated publishing capabilities to schedule jobs and support continuous integration for every sprint. Automated build tools shall be in compliance with the approved list from the One-VA TRM and code shall be demonstrable and stable enough to be promoted to another environment without issue by evidence of the status of tests and results in the Rational Tools.
8. Initiate and facilitate a Sprint Retrospective at the end of the Sprint to capture team performance lessons learned.

A7.0 TESTING

The contractor shall adopt agile best practices for integration testing into each agile development sprint and build. The contractor shall populate their Test Strategy section of the test plan in VA's implementation of Rational Quality Manager tool within 15 days after technical kickoff meeting. The contractor shall conduct tests (e.g. unit, functional, accessibility, system, reliability, usability, interoperability, regression, security, performance) throughout the development lifecycle (e.g. user story, sprint, build, release) using industry best practices of continuous integration methods and automated regression testing utilities using One-VA Technical Reference Model (TRM) approved tools. The contractor shall conduct testing related to non-functional requirements, (e.g. load, performance, installation, back-out, and rollback).

The contractor shall provide test plan data in the Rational Quality Manager following the templates and data requirements appropriate for each test purpose appropriate to each phase of development. The contractor shall provide test results in the Rational Quality Manager which is the final piece of data that completes the Requirements Traceability Matrix (RTM). COR/VA PM acceptance will occur through the Rational Quality Manager approval process.

The contractor shall support the security, accessibility, performance, technical standards, architectural compliance, user acceptance and initial operational capability tests, audits, and reviews. Security scanning is done by multiple methods and is done multiple times throughout the course of a project with methods such as infiltration testing (WASA), code analysis tools (Fortify), etc. Accessibility reviews are performed through a variety of tool based and manual reviews, able to scan web applications and other technologies used for user interfaces. Performance testing is done through load testing and technical analysis of capacity planning data submitted by the project team. Architectural compliance assessments are done through submission of design materials to confirm compliance with allowed EA.

Addendum A

The contractor shall ensure all test and compliance review planning and execution details and their testing and compliance results are entered and maintained in Rational Quality Manager and under version control in Rational Team Concert. Specifically test management data and artifacts include such items as scripts, configurations, utilities, tools, plans and results. The contractor shall ensure that results of all assessments of the project performed by the contractor or by VA offices are consolidated into Rational for planning and status reporting.

When a defect is identified during testing, the contractor shall log it in Rational, selecting the appropriate severity level. The contractor shall support the Project Manager for prioritizing the defect in the sprint backlog. Based on a prioritization the defect could be entered into the current sprint or entered into the backlog.

The contractor shall ensure Rational data is up-to-date on a daily basis so that VA stakeholders can access accurate and timely status.

A8.0 RELEASE SUPPORT

The VIP Release Process is conducted during the build and development cycle by one or more assigned Release Agents, who perform frequent, regular reviews of required and appropriately linked product data in the mandated repositories. The Release Agents also provide timely feedback to the product team concerning the status of the product data and the status of the team's compliance with the VIP Release Process. The contractor shall support OI&T's single VIP Release process.

The POLARIS calendaring process and tool will be used to track software installations, hardware replacements, system upgrades, patch release and implementation, special works in progress, and other deployment events in the VA production environment. The contractor shall provide data for populating and updating the POLARIS calendaring process for each release and deployment.

The contractor shall develop and finalize the Production Operations Manual (POM) and/or the Technical Manual, depending on the product being produced. The POM or Technical Manual shall include regular maintenance and operations information, Responsibility, Accountability, Consulted, and Informed (RACI) information, process flowcharts, dataflow diagrams, key monitoring indicators, and troubleshooting information.

The contractor shall develop the Deployment and Installation Guide which includes back-out and rollback procedures.

The contractor shall develop a User Manual which addresses procedural information for the business users on daily operational use of the software.

The contractor shall hold test site calls with VA staff to include Release Coordinators and VIP Release Agents once the product is approved for IOC production testing.

Addendum A

The contractor shall provide all required documentation and receive approval for Authority to Operate (ATO) as specified in EPMO Website.

A9.0 RELEASE AND DEPLOYMENT SUPPORT

In accordance with the VIP Guide, Release and deployment support begins upon successful completion of National Deployment for the first release and ends after the warranty period of the final release is completed.

For a period of 90 days after the final National Deployment release is completed the contractor shall warrant all requirements and deliverables in the scope of this contract. Defects may be identified by the Government and its designees, to include all necessary personnel as designated by the COR. For each defect identified, the contractor shall triage the defect in accordance with the table below, identify a resolution for the defect, and provide a plan for resolution, including timeline and impacts to the code and updates to Rational. Following COR approval of the contractor defect resolution plan, the contractor shall execute the approved plan.

Code	Tier 2 Initial Response to Customer	Tier 2 escalates to Tier 3 for initial contact	Tier 3 response to Tier 2	Tier 2 requests updates from Tier 3 based on SLA resolution	Resolution Time – based on SLA from time incident was initially reported
1 – Critical	15 minutes	0-15 minutes	15 minutes	On call until issue resolved or hourly status check	0-2 business hours
2 – Serious	1 hour	30 minutes	1 hour	On call until issue resolved or hourly status check	2-4 business hours
3 – Moderate	4 hours	1 hour	4 hours	Daily	4-8 business

Addendum B

ADDENDUM B – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

B1.0 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 PM, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

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

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.

B2.0 VA Enterprise Architecture (EA) Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA EA, available at <http://www.ea.oit.va.gov/index.asp> in force at the time of

Addendum B

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.

B2.1. 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

B3.0 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.

B3.1. Section 508 – Electronic and Information Technology (EIT) Standards

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

Addendum B

- ☒ § 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

B3.2. 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.

B3.3. 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.

B3.4. Acceptance and Acceptance Testing

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

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

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

B4.0 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.

Addendum B

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.

B5.0 Confidentiality and Non-Disclosure

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

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

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

Addendum B

regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this contract and its subparts and appendices.

4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the contractor has a responsibility to ask the VA CO.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any contractor facilities according to VA-approved guidelines and directives. The contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
 - a. The use of "thumb drives" or any other medium for transport of information is expressly prohibited.
 - b. Controlled access to system and security software and documentation.
 - c. Recording, monitoring, and control of passwords and privileges.
 - d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
 - e. VA, as well as any contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
 - f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
 - g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)."
 - h. Contractor does not require access to classified data.
8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/contractor relationships.
9. VA Form 0752 shall be completed by all contractor employees working on this contract, and shall be provided to the CO before any work is performed. In the case that contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

Addendum B

B6.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

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

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

1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).
2. Provide/use the purchasing specifications listed for FEMP designated products at https://www4.eere.energy.gov/femp/requirements/laws_and_requirements/energy_star_and_femp_designated_products_procurement_requirements. 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. 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 C

ADDENDUM C – 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

A. 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.

B. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

1. 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.
2. 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.
3. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISIP) 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 VA 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.
4. 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.
5. The contractor or subcontractor must notify the CO immediately when an

Addendum C

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

C. VA INFORMATION CUSTODIAL LANGUAGE

1. Information made available to the contractor or subcontractor by VA for the performance or administration of this contract or information developed by the contractor/subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of VA. This clause expressly limits the contractor/subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).
2. VA information should not be co-mingled, if possible, with any other data on the contractors/subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the contractor must ensure that VA information is returned to VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on-site inspections of contractor and subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.
3. Prior to termination or completion of this contract, contractor/subcontractor must not destroy information received from VA, or gathered/created by the contractor in the course of performing this contract without prior written approval by VA. Any data destruction done on behalf of VA by a contractor/subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the contractor that the data destruction requirements above have been met must be sent to the VA CO within 30 days of termination of the contract.
4. The contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.
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

Addendum C

storage media for restoration in case any electronic equipment or data used by the contractor/subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

6. If VA determines that the contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.
7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.05, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.
8. The contractor/subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.
9. The contractor/subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA minimum requirements. VA Configuration Guidelines are available upon request.
10. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor/subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA prior written approval. The contractor/subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA CO for response.
11. Notwithstanding the provision above, the contractor/subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the contractor/subcontractor is in receipt of a court order or other requests for the above mentioned information, that contractor/subcontractor shall immediately refer such court orders or other requests to the VA CO for response.
12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require Assessment and Authorization (A&A) or a Memorandum of Understanding-Interconnection 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.

D. 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

Addendum C

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 VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*, and the TIC Reference Architecture). 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, *Implementation of Privacy Threshold Analysis and 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 11 configured to operate on Windows 7 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, *Risk Management Framework for VA Information Systems – Tier 3: VA 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

Addendum C

- 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 (c), 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 upon 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

Addendum C

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 CO and the VA Assistant Secretary for Office of Information and Technology.

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

1. 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 in accordance with the TIC Reference Architecture and reviewed and approved by VA prior to implementation.
2. 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.
3. Outsourcing (contractor facility, contractor equipment or contractor staff) of systems or network operations, telecommunications services, or other managed services requires A&A of the contractor's systems in accordance with VA Handbook 6500.3, Assessment, Authorization and Continuous Monitoring of VA Information Systems 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.
4. 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 CO 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

Addendum C

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 A&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 A&A would be necessary.

5. 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.
6. 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, PWS, or contract. All of the security controls required for Government furnished equipment (GFE) must be used 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.
7. 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.
8. 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:
 - a. Vendor must accept the system without the drive;
 - b. 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
 - c. VA must reimburse the company for media at a reasonable open market

Addendum C

replacement cost at time of purchase.

- d. 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;
 - 1) 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
 - 2) 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.
 - 3) 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.

F. SECURITY INCIDENT INVESTIGATION

1. 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.
2. 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.
3. 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.
4. 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

Addendum C

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.

G. LIQUIDATED DAMAGES FOR DATA BREACH

1. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the contractor/subcontractor processes or maintains under this contract. However, it is the policy of VA to forgo collection of liquidated damages in the event the Contractor provides payment of actual damages in an amount determined to be adequate by the agency.
2. 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.
3. Each risk analysis shall address all relevant information concerning the data breach, including the following:
 - a. Nature of the event (loss, theft, unauthorized access);
 - b. Description of the event, including:
 - i. date of occurrence;
 - ii. data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
 - c. Number of individuals affected or potentially affected;
 - d. Names of individuals or groups affected or potentially affected;
 - e. 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;
 - f. Amount of time the data has been out of VA control;
 - g. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
 - h. Known misuses of data containing sensitive personal information, if any;
 - i. Assessment of the potential harm to the affected individuals;
 - j. Data breach analysis as outlined in 6500.2 Handbook, Management of Breaches Involving Sensitive Personal Information, as appropriate; and

Addendum C

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

H. 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.

I. TRAINING

1. 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:
 - a. 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.
 - b. 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 CO for inclusion in the

Addendum C

solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]

2. The contractor shall provide to the CO and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.
3. 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.

Addendum C

SCHEDULE FOR DELIVERABLES

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

Task	Deliverable ID	Deliverable Description
5.1	A	Staffing Assignment Worksheet Due thirty (30) days after receipt of order (ARO) and updated as necessary thereafter. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1	B	TMS Certificates for IBM Rational Tools Courses Due thirty (30) days after ARO. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1	C	VA Privacy and Information Security Awareness and Rules of Behavior Training Certificate Due thirty (30) days after ARO and annually thereafter. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1	D	Signed Contractor Rules of Behavior Due thirty (30) days after ARO and annually thereafter. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1	E	VA HIPPA Certificate of Completion Due thirty (30) days after exercise ARO and annually thereafter.. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1	F	Contractor Project Management Plan Due thirty (30) days ARO and updated as necessary thereafter. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1	G	Monthly Progress Report Due thirty (30) days after ARO and updated monthly thereafter. Electronic submission to: VA PM, COR, CO.

Addendum C

		<p>Inspection: destination</p> <p>Acceptance: destination</p>
5.1.1		<p>Kick-off meeting agenda and meeting minutes</p> <p>Agenda due ten (9) days ARO, minutes due 3 days after meeting.</p> <p>Electronic submission to: VA PM, COR, CO.</p> <p>Inspection: destination</p> <p>Acceptance: destination</p>
5.2.8	A	<p>Signature Informed Consent Compliant Software</p> <p>Due immediately ARO and updated as releases are available and approved.</p> <p>Electronic submission to: VA PM, COR, CO.</p> <p>Inspection: destination</p> <p>Acceptance: destination</p>
5.2.8	B	<p>PIV Sign-On Compliant Software</p> <p>Due 90 days after ARO.</p> <p>Electronic submission to: VA PM, COR, CO.</p> <p>Inspection: destination</p> <p>Acceptance: destination</p>
5.2.8	C	<p>Quarterly Update Usage Reports</p> <p>Due thirty (30) days ARO and updated monthly.</p> <p>Electronic submission to: VA PM, COR, CO.</p> <p>Inspection: destination</p> <p>Acceptance: destination</p>
5.2.8	D	<p>Quarterly Consent Form Updates</p> <p>Due thirty (30) days ARO and updated every 90 days.</p> <p>Electronic submission to: VA PM, COR, CO.</p> <p>Inspection: destination</p> <p>Acceptance: destination</p>
5.2.8	E	<p>Graphic Report</p> <p>Due thirty (30) days ARO and updated as releases become available.</p> <p>Electronic submission to: VA PM, COR, CO.</p> <p>Inspection: destination</p> <p>Acceptance: destination</p>
5.2.8	F	<p>VA 508 Compliance Certification</p> <p>Due sixty (60) days ARO and updated as releases become commercially available.</p> <p>Electronic submission to: VA PM, COR, CO.</p> <p>Inspection: destination</p> <p>Acceptance: destination</p>
5.3	F	<p>Quarterly Support Call Logs</p> <p>Due 90 (90) days ARO and updated quarterly..</p> <p>Electronic submission to: VA PM, COR, CO.</p> <p>Inspection: destination</p> <p>Acceptance: destination</p>
5.5.1 (Optional Task 1)	A	<p>Product Configuration Management Plan</p> <p>Due thirty (30) days after exercise of option.</p>

Addendum C

		Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.5.1 (Optional Task 1)	B	Version Description Document Due thirty (30) days after exercise of option. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.5.1 (Optional Task 1)	C	VA Compatible version of Electronic Informed Consent Web-Based COTS Software Due one hundred twenty (120) days after exercise of option. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.5.1 (Optional Task 1)	D	Section 508 Compliance Certification Due sixty (60) days after exercise of option. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.5.1 (Optional Task 1)	E	Test Strategy Data Input into Rational Due thirty (30) days after exercise of option. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.5.1 (Optional Task 1)	F	Test Plan and Test Execution Data Input into Rational Due thirty (30) days after exercise of option. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.5.1 (Optional Task 1)	G	Requirements Traceability Matrix (RTM) in Rational Due thirty (30) days after exercise of option. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.5.1 (Optional Task 1)	H	Production Operations Manual (POM) and/or Technical Manual Due thirty (90) days after exercise of option. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.5.1 (Optional Task 1)	I	Deployment and Installation Guide Due thirty (90) days after exercise of option. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.5.1 (Optional Task 1)	J	User Manual Due thirty (90) days after exercise of option.

Addendum C

		Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.4 (Optional Task 2)	A	VA Training Module Scripts and Training Module Screen Shot Mock Ups Due thirty (30) days after exercise of option. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.4 (Optional Task 2)	B	VA Users Training Module on TMS Due one hundred twenty (120) days after exercise of option. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.4 (Optional Task 2)	C	VA Administrator Training Module on TMS Due one hundred twenty (120) days after exercise of option. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination