

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		BPA NO.	1. CONTRACT ID CODE	PAGE 1	OF PAGES 49
2. AMENDMENT/MODIFICATION NUMBER A00001		3. EFFECTIVE DATE		4. REQUISITION/PURCHASE REQ. NUMBER	
5. PROJECT NUMBER (if applicable)		6. ISSUED BY CODE		7. ADMINISTERED BY (If other than Item 6) CODE	
Department of Veterans Affairs Technology Acquisition Center 23 Christopher Way Eatontown NJ 07724		Department of Veterans Affairs Technology Acquisition Center 23 Christopher Way Eatontown NJ 07724			
8. NAME AND ADDRESS OF CONTRACTOR (Number, street, county, State and ZIP Code) To all Offerors/Bidders		(X)		9A. AMENDMENT OF SOLICITATION NUMBER VA118-17-R-1804	
		X		9B. DATED (SEE ITEM 11)	
				10A. MODIFICATION OF CONTRACT/ORDER NUMBER	
				10B. DATED (SEE ITEM 13)	
CODE		FACILITY CODE			

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

- ☒ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☒ is not extended.
- Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:
- (a) By completing Items 8 and 15, and returning 1 copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

**13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS,
IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.**

CHECK ONE	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
	D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor ☐ is not, ☐ is required to sign this document and return _____ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

See Continuation Page

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)	
15B. CONTRACTOR/OFFEROR _____ (Signature of person authorized to sign)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA BY _____ (Signature of Contracting Officer)	16C. DATE SIGNED

CONTINUATION PAGE

The purpose of this Amendment A00001, to Request for Proposal (RFP) VA118-17-R-1804 titled “National Dialysis Electronic Health Record (EHR) Solution,” is as follows:

1. Section B.7 Performance Work Statement
 - a. Paragraph 4.0 Ordering Period – Removed sentence “Options shall not exceed 24 months from the expiration of the contract ordering period.”
 - b. Paragraph 5.3.3 Reference Materials – Included, “including installation guides for all interfaces” to the Installation Guide deliverable.
2. Section C – Contract Clauses
 - a. Section C.6 52.216-22, Indefinite Quantity (OCT 1995) - Replaced “24 months” in paragraph (d) with “12 months”.
 - b. Section C.8 52.217-9, Option to Extend the Term of the Contract (MAR 2000) – Replaced paragraph (c) with “The total duration of this contract, including the exercise of any options under this clause, shall not exceed 72 months.”
3. Except as provided herein, all other terms and conditions of RFP VA118-17-R-1804 remain unchanged and in full force and effect.

SECTION B – CONTINUATION OF SF30 BLOCKS

B.7 PERFORMANCE WORK STATEMENT



**DEPARTMENT OF VETERANS AFFAIRS
Veterans Health Administration
Specialty Care Services
National Dialysis Electronic Health Record (EHR) Solution Contract**

**Date: 1/24/2016
TAC-16-29607
PWS Version Number: 1.6**

1.0 BACKGROUND

The Department of Veterans Affairs (VA), Veterans Health Administration (VHA) provides health care benefits and services to Veterans of the United States. Dialysis is a life-saving treatment that is required when the loss of kidney function becomes permanent. There are over 100 VA facilities that provide dialysis to approximately 10,000 Veterans each year.

VHA lacks a uniform mechanism for capture and reporting of dialysis data. This has resulted in incomplete and inconsistent data capture and reporting among VA dialysis facilities.

Specifically, VA dialysis facilities lack the necessary software for electronic reporting to the Centers for Medicare and Medicaid (CMS) mandated web-based dialysis quality collection system known as CROWNWeb (Consolidated Renal Operations in a Web-Enabled Network). Additionally, support for the software (FMiS) that the majority of VA facilities use to document dialysis treatments was discontinued on March 31, 2016.

VHA requires a dialysis electronic health record (EHR) solution for VA facilities that provide dialysis services throughout the United States; including Alaska, Hawaii, and Puerto Rico. The requirement includes the dialysis EHR solution, all associated hardware and software, installation, testing, training, maintenance, and technical support. The proposed acquisition will provide customers throughout VA with a means of procuring a standardized dialysis EHR solution to satisfy the needs for providing dialysis services to Veterans. Providing a single award Indefinite Delivery Indefinite Quantity (IDIQ) contract for VA organizations to fulfill their requirements will enable VA to quickly and efficiently acquire a standardized dialysis EHR solution that meets the customer's minimum need and continues to ensure quality dialysis services are provided to Veterans.

2.0 APPLICABLE DOCUMENTS

Below is a list of reference documents associated with this Performance Work Statement. The Contractor shall comply with the following documents as applicable:

1. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002"
2. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
3. FIPS Pub 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013
4. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
5. VA Directive 0710, "Personnel Security and Suitability Program," June 4, 2010, <http://www.va.gov/vapubs/>
6. VA Handbook 0710, Personnel Security and Suitability Security Program, May 2, 2016, <http://www.va.gov/vapubs>
7. VA Directive and Handbook 6102, "Internet/Intranet Services," July 15, 2008
8. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
9. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
10. 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
11. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004

12. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, 2012
13. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” March 10, 2015
14. VA Handbook 6500.1, “Electronic Media Sanitization,” November 03, 2008
15. VA Handbook 6500.2, “Management of Breaches Involving Sensitive Personal Information (SPI),” October, 28, 2015
16. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring Of VA Information Systems,” February 3, 2014
17. VA Handbook 6500.5, “Incorporating Security and Privacy in System Development Lifecycle”, March 22, 2010
18. VA Handbook 6500.6, “Contract Security,” March 12, 2010
19. VA Handbook 6500.8, “Information System Contingency Planning”, April 6, 2011
20. Office of Information and Technology (OI&T) ProPath Process Methodology (reference process maps at <http://www.va.gov/PROPATH/Maps.asp> and templates at <http://www.va.gov/PROPATH/Templates.asp>)
21. One-VA Technical Reference Model (TRM) (reference at <http://www.va.gov/trm/TRMHomePage.asp>)
22. VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment, October 15, 2014
23. VA Handbook 6508.1, “Procedures for Privacy Threshold Analysis and Privacy Impact Assessment,” July 30, 2015
24. VA Directive 6300, Records and Information Management, February 26, 2009
25. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
26. OMB Memorandum, “Transition to IPv6”, September 28, 2010
27. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015
28. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 24, 2014
29. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
30. OMB Memorandum 05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005
31. 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
32. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
33. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
34. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
35. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
36. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
37. NIST SP 800-157, Guidelines for Derived PIV Credentials, December 2014
38. NIST Special Publication 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012

39. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
40. VA Memorandum, VAIQ #7100147, Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12), April 29, 2011 (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>)
41. 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>)
42. 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>)
43. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, Department of Homeland Security, October 1, 2013, https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf
44. OMB Memorandum M-08-05, “Implementation of Trusted Internet Connections (TIC), November 20, 2007
45. OMB Memorandum M-08-23, Securing the Federal Government’s Domain Name System Infrastructure, August 22, 2008
46. VA Memorandum, VAIQ #7497987, Compliance – Electronic Product Environmental Assessment Tool (EPEAT) – IT Electronic Equipment, August 11, 2014 (reference Document Libraries, EPEAT/Green Purchasing Section, <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=552>)
47. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
48. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
49. Executive Order 13693, “Planning for Federal Sustainability in the Next Decade”, dated March 19, 2015
50. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
51. VA Directive 0058, “VA Green Purchasing Program”, July 19, 2013
52. VA Handbook 0058, “VA Green Purchasing Program”, July 19, 2013
53. Office of Information Security (OIS) VAIQ #7424808 Memorandum, “Remote Access”, January 15, 2014, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
54. VA Memorandum, “Implementation of Federal Personal Identity Verification (PIV) Credentials for Federal and Contractor Access to VA IT Systems”, (VAIQ# 7614373) July 9, 2015, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
55. VA Memorandum “Mandatory Use of PIV Multifactor Authentication to VA Information System” (VAIQ# 7613595), June 30, 2015, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
56. VA Memorandum “Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges” (VAIQ# 7613597), June 30, 2015; <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
57. “Veteran Focused Integration Process (VIP) Guide 1.0”, December, 2015, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>
58. “VIP Release Process Guide”, Version 1.4, May 2016, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4411>
59. “POLARIS User Guide”, Version 1.2, February 2016, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4412>

60. Consolidated Renal Operations in a Web-enabled Network (CROWNWeb) Business and Reporting Requirements, Business Rules, and Kidney Data Definitions
<http://mycrownweb.org/help/release-documents/kidney-data-dictionary/>
61. CROWNWeb Data Submission Schedule
<http://mycrownweb.org/help/accessing-crownweb/crownweb-data-submission-provider-schedule/>
62. National Renal Administrators Association (NRAA) Health Information Exchange (HIE) for Reporting to CROWNWeb
<http://www.renalexchange.com/nraa-hie-for-crownweb/>
63. [VHA Handbook 1153.01, "Use of Centers for Medicare and Medicaid \(CMS\) and United States Renal Data Systems \(USRDS\) Data in the Veterans Health Administration," April 15, 2016](#)

3.0 SCOPE OF WORK

The Contractor shall execute this contract for providing all aspects of the dialysis EHR solution including all hardware, software, interfaces, configuration, installation, testing, training, maintenance, and support as specified in this PWS and in accordance with individual task orders (TO). Hardware does not refer to the dialysis machines or VA computer workstations (refer to Section 6.1). All software furnished under this Contract shall be perpetual licenses and include all upgrades, version changes, and/or updates. The Contractor shall ensure that the dialysis EHR solution operates as defined in Section 5. Maintenance and technical support shall include scheduled maintenance/repairs, unscheduled maintenance, preventative maintenance, and maintenance of the interfaces for the duration of this contract.

4.0 PERFORMANCE DETAILS

This is a single award IDIQ contract from which firm fixed priced task orders shall be issued. Task orders will be issued by the Technology Acquisition Center (TAC).

4.1 ORDERING PERIOD

The ordering period, shall be for five years, i.e. 60 months. Individual task orders may include options for extended terms and increased quantities. ~~Options shall not exceed 24 months from the expiration of the contract ordering period.~~

4.2 PLACE OF PERFORMANCE

Products and services ordered under this contract shall be delivered to and installed at VA locations throughout all 50 states as well as Puerto Rico and Washington D.C. as specified in individual task orders. Incidental services, such as training or on-site maintenance, shall be provided at these locations as necessary. Work may be performed at Contractor facilities or remote locations other than Contractor facilities with prior concurrence from the Contracting Officer Representative (COR). Products and services shall be available to any VA facility that provides dialysis. The location of VA facilities that currently provide dialysis is provided in Addendum C (Note: List subject to change).

4.3 TRAVEL

Travel shall be in accordance with individual TO requirements. The Government anticipates travel under this effort to perform the tasks required in the PWS and individual task orders. All estimated travel costs should be included in the firm-fixed price line items. Travel costs will not be directly reimbursed by the Government as a separately priced item.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall provide a dialysis EHR solution that meets the following requirements:

5.1 DIALYSIS EHR SOLUTION REQUIREMENTS

5.1.1 SOFTWARE AND HARDWARE

1. The Contractor shall provide the dialysis EHR solution and all associated licenses, applications, operating systems, software, and hardware necessary to meet the requirements defined in section 5.1 unless otherwise noted. The cost of ancillary items such as cables shall be included in the cost of the dialysis EHR solution and shall not be priced separately unless otherwise noted.
2. The Contractor shall provide all servers and associated server licenses, applications, shipping, and operating systems (as requested by the ordering facility) to support the dialysis EHR solution. The Contractor shall ensure continued server compatibility with the dialysis EHR solution. The cost of the server and associated server licenses, applications, shipping, and operating systems shall be priced separately. The Contractor shall provide pricing for physical and virtual servers. VHA facilities may elect to procure physical or virtual servers.
3. The Contractor shall provide all serial to Ethernet converters and associated cables required for operation of the dialysis EHR solution (as requested by the ordering facility). The cost of the serial to Ethernet converter shall be priced separately.

5.1.2 VISTA INTERFACE

1. The dialysis EHR solution shall interface with the Veterans Health Information Systems and Technology Architecture (VistA) at each ordering facility. VistA is VA's EHR. The interface shall be Health Level 7 (HL7) 2.5 compliant.
2. The dialysis EHR solution shall be capable of continuously acquiring all data described below from VistA and importing the data into the dialysis EHR solution in a useable format. Data shall be available real-time and retrospectively. Data shall be exchanged at a minimum uni-directionally from VistA to the EHR unless otherwise noted.
 - a. Time and date
 - 1) Time and date shall be synchronized with VistA.
 - b. Patient identification and information
 - 1) VistA identity management procedures shall be maintained.
 - 2) Patient demographics such as name, age, date of birth, social security number, mailing address, personal contacts, employment history, insurance providers.
 - 3) Problem list and diagnosis (problem list, International Classification of Diseases (ICD)-10 code, primary and secondary diagnoses, etc.)
 - 4) Allergies (pharmaceutical and non-pharmaceutical)
 - 5) Advanced directives and code status such as Crisis, Warnings, Allergies, and Advanced Reactions and Directives (CWAD); Do Not Attempt Resuscitation (DNAR/DNR) Order; State Authorized Portable Orders (SAPO); legal guardianship status.
 - c. Orders and results
 - 1) Laboratory orders and results
 - A. Shall provide two-way bi-directional transmission of laboratory orders between the dialysis EHR solution and VistA. Shall have a laboratory interface that allows users to order labs within the dialysis EHR solution.

- The dialysis EHR solution shall transmit lab orders to VistA. Lab orders in VistA shall be transmitted to the dialysis EHR solution.
- B. Shall provide bi-directional transmission of laboratory results from VistA to the dialysis EHR solution.
- C. Shall allow users to define the lab orders and results that are transmitted between the dialysis EHR solution and VistA.
- D. Shall contain a drop down menu/pick list of labs, a catalog name search, and frequently ordered labs.
- E. Shall associate received lab results from VistA with the original lab order. Shall accept unsolicited observation result (ORU) messages.
- F. Shall report lab results. Shall clearly display units, reference ranges, out of range, and critical values with lab results. Shall display microbiology and blood bank including entire culture reports and antibiotic sensitivities with lab results. All parent/child reports shall be included with each lab result update.
- G. Shall determine if received lab results are part of a calculated lab value, and if so calculate the lab value. Shall automatically calculate pertinent dialysis management values based on lab data (i.e. Kt/v).
- H. Shall display lab results in logical categories (e.g., Complete Blood Count (CBC) panel).
- 2) Medication orders, schedule, and administration
 - A. Shall transmit medication orders, schedule, and administration from VistA to the dialysis EHR solution. Bar Code Medication Administration (BCMA) is the application within VistA used to document medication administration.
 - B. Shall be capable of receiving data from BCMA and automatically populating data from BCMA into the patient record including all medications administered to the patient during dialysis.
- 3) Shall transmit all dialysis patient records generated in the dialysis EHR solution (such as the hemodialysis flowsheet and progress notes) to VistA as a Computerized Patient Record System (CPRS) note.

5.1.3 DIALYSIS MACHINE INTERFACE

1. The dialysis EHR solution shall interface with all dialysis machines approved by the Food and Drug Administration (FDA) for use in the United States.
2. For informational use, the dialysis machines and associated software currently in use at VA are listed below. The Contractor shall not be responsible for connecting the dialysis machines to the VA network as this will be performed by OI&T at each facility. Additionally, the scope of this contract includes dialysis machines that VA may purchase in the future.
 - a. Machine: Phoenix X36; Software: Exalis
 - b. Machine: Fresenius: 2008K, 2008K2, 2008T, and H models; Software: FMiS
 - c. Machine: B. Braun: Dialog+; Software: Dialog Reporter
3. The dialysis EHR solution shall be capable of continuously acquiring all data (measurements, settings, and calculations) from the dialysis machine in real-time at the maximum rate available. Data extraction shall occur at least every 5 minutes. Data shall be in useable format and available real-time and retrospectively.

5.1.4 SOFTWARE MEDIATED WORKFLOWS

1. The dialysis EHR solution shall have built-in Windows standard copy and paste functionality.
2. Patient selection and identification
 - a. The dialysis EHR solution shall provide a patient worklist that interfaces with VistA.
 - b. The dialysis EHR solution shall prominently display patient name and last four of the social security number on every relevant page (including all pages of the hemodialysis flowsheet, progress notes, etc.).
3. The dialysis EHR solution shall be capable of automatically generating a hemodialysis flowsheet (i.e. chart) of each dialysis treatment using data acquired from the dialysis machine, VistA, and inputted by the user. Information requiring user input of data shall be clearly identified (i.e. asterisk). The flowsheet shall contain the following:
 - a. Connecting Screens
 - 1) Shall maximize pre-population and automatic import of data. Shall have built-in functionality that allows the user to stop/copy/new orders. For example, a user could create a new order using the data elements from the old record and edit only the items requiring modification. Pre and post dialysis signs captured by dialysis machines with blood pressure cuffs shall be automatically imported.
 - 2) Shall have built-in sign off validation requirements throughout the flowsheet that are configurable. Shall require the user to indicate that he/she has completed all checks and reviewed order information. Shall only allow sign off once all topics within the flowsheet are complete.
 - b. Treatment Orders and Review
 - 1) Shall allow input of the dialysis treatment order into the dialysis EHR solution.
 - 2) Shall include customizable long-term and daily hemodialysis orders.
 - 3) Shall automatically load and display all medication, lab, and other orders/reminders relevant for each treatment. Shall not require user data entry.
 - 4) Shall differentiate between required and pro re nata (PRN) medications.
 - 5) Shall display missed medications, labs, and orders from prior dates.
 - c. Machine Checks
 - 1) Shall automatically import data documenting that the dialysis machine passed or failed all tests at the start of treatment.
 - d. Structured Pre-Treatment Assessment and Vitals
 - 1) Shall include a list of questions with check list/drop down type of documentation requiring one keystroke. Shall allow configuration of assessment questions.
 - 2) Shall display prior treatment vitals for comparison while documenting pre-treatment vitals.
 - 3) Shall include dynamic data checks comparing entry to patient attributes such as height, weight, and blood flow rate. For example, if the user enters the patient's weight at 200 pounds (lb.) and the previous treatment was 90 lb.; the dialysis EHR solution shall warn the user that the weight does not fall within the threshold for that patient.
 - e. Treatment Observations and Charting

- 1) Shall allow the user to easily view required documentation.
- 2) Shall continuously track treatment monitoring data based on configurable selections made by the user.
- 3) Shall allow the user to access the dialysis EHR solution progress note with one click to chart treatment observations.
- 4) Shall allow the user to document all active medication and lab orders as: given/drawn or not given/not drawn. Shall require the user to input reason for medications/labs that are not given/not drawn.
- 5) Shall have pre-defined selections/drop-down menus for charting adverse events/complications. Shall include ability to pre-define events and protocols within the charting form.
- f. Structured Post-Treatment Assessment and Vitals
 - 1) Shall include a list of discharge assessment questions with check list/drop down type of documentation requiring one keystroke. Functionality shall be the same as the pre-treatment assessment screen.
 - 2) Shall display pre and post answers and treatment vitals for comparison.
- g. Closing Flowsheet
 - 1) Shall require completion and sign off of each section of the flowsheet prior to closing. Shall alert the user of incomplete charting when closing session.
- h. Management Screen
 - 1) Shall include a screen that allows the user to review the status of all patients scheduled for the day.
4. The dialysis EHR solution shall include progress notes, templates, and forms to document patient status.
 - a. The dialysis EHR solution shall include: a comprehensive and searchable library of standard templates and forms; pre-loaded progress note templates for clinical documentation; pre-loaded short-term and long-term care plan templates that adhere to CMS End Stage Renal Disease (ESRD) Conditions for Coverage (CfC); pre-loaded forms that mimic CMS ESRD CfC required forms including CMS Forms 2728 and 2746; vascular access templates that allow documentation of: creation/failure, location, complications, and recirculation; and time-out templates.
 - b. Templates, forms, and progress notes shall: be able to be configured by the user; pre-populate data from the patient's record; maximize the use of drop-down menus; include the ability for the user to annotate data; maintain an audit trail of data that is user-corrected or automatically corrected; and include ability to be printed by the user.
5. The dialysis EHR solution shall be capable of automatically integrating lab results and medications for use in Quality Assurance and Performance Improvement (QAPI).

5.1.5 ALERTS

1. The dialysis EHR solution shall display alerts in an easily comprehensible format (e.g., color coded icon).
2. The dialysis EHR solution shall display a 'connection interrupted' indicator obvious to the user within five minutes of a communication interruption with any interface.
3. The dialysis EHR solution shall continue to accept and store data even when connection to VistA is interrupted. Shall have the ability to re-send data to VistA when communication is restored.

5.1.6 CALCULATIONS, REPORTS, AND DASHBOARDS

1. Calculations
 - a. Shall accept calculated values from all interfaces.
 - b. Shall have pre-loaded ability to automatically calculate treatment and patient indicators including:
 - 1) Kt/V (dialysis dose). Minimum requirement is Daugirdas II Kinetic second generation logarithmic equation.
 - 2) Urea Reduction Ratio (URR)
 - 3) Protein Catabolism Rate Normalized (PCRN)
 - 4) Weight differentials. Delta weight from one treatment to the next and the delta weight during treatment.
 - 5) Corrected calcium
 - 6) Ultrafiltration (UF)
 - 7) QAPI statistics (means, outliers,)
 - c. Shall display calculated indicators on appropriate screens/reports.
2. Reports
 - a. Shall include pre-loaded reports and shall have the capability of generating user-defined reports at the patient and clinic level.
 - b. Shall have the ability to generate reports comparing indicators from different time periods.
 - c. Reports (including customized reports) shall be highly-formatted and have an intuitive design interface. Shall allow export of reports into multiple standard formats such as Portable Document Format (PDF), Hyper Text Markup Language (HTML), and Excel.
 - d. Shall have the capability of generating all CROWNWeb required reports. Refer to Section 2.0 Applicable Documents.
 - e. Shall have the capability of generating QAPI reports addressing all standard dialysis quality metrics, including dialysis solute removal, anemia and bone disease management, vascular access care, and infection prevention and tracking reports.
 - f. Shall have the capability of generating lab reports. Shall have decision logic that monitors and integrates incoming lab, medication, and clinical data streams. When a lab value is reported to the dialysis EHR solution from VistA, the dialysis EHR solution shall generate a report that lists all patients whose lab value is an outlier (as specified by the user). The report shall identify the absolute number of patients and percentage of total treating patients. All other lab values and clinical data including medication doses that are pertinent to the outlying lab value shall be pulled automatically and collated into a report. The report shall allow the user to easily view all the variables that need to be adjusted in order to correct the outlying value. The report shall identify the appropriate adjustment in each of the variables and allow the user to make adjustments identified in the report in the patient's orders from the same report screen.
 - g. Shall have the capability of generating medication reports including: medications to be reviewed, active medications, medication orders, Erythropoietin (EPO) administration, medications administered during treatment session, medication given history, non-ESRD medication orders audit, vaccination audit, and bone management .
 - h. Shall have the capability of generating a portfolio of reports such as those regarding: unverified and un-carried orders; patient demographics; problem list;

patient history; modality history; monthly assessment; transplant assessment; vascular access; infection monitoring; anemia monitoring; nutrition record; consultation report; care plan; progress note summary; patient education; and vaccinations.

- i. Shall have the capability of generating management reports regarding: patient/staff scheduling, scheduled treatments, treatment duration and variation, missed treatments, treatment summary, workload, facility census, and transfers or deaths on a month by month basis.
 - j. Shall have the capability of generating customized reports from existing reports or from scratch based on user-defined parameters.
 - k. Shall allow users to query data, design, and generate reports on a user-defined schedule.
3. Dashboards
- a. Shall include pre-loaded clinical dashboards at the patient and clinic level that users may modify.
 - b. Shall display in graphical and tabular format key data and performance indicators and identify outliers. Graphical presentation for patients shall be in the form of trends over time. Graphical presentation for the patient population shall be in the form of pie charts indicating patient distributions.
 - c. Shall have the ability to generate patient-specific trend analyses that enable quick ranking of patients most at risk.
 - d. Shall include the ability to compare indicators from different time periods.

5.1.7 USER INTERFACE

1. Shall allow users to view all relevant clinical data on a single screen, quickly document notes using template-driven check boxes, and sign orders. Shall allow users to access a function with two clicks or less and exercise a function with one click.
2. Shall have an implicit user interface including: colors, icons, graphs, pick lists, drop down menus, free form text, notes, forms, point and click, drop and drag, copy and paste, and other normalized Word-type capabilities.
3. Shall minimize data entry and keystrokes. Shall have single point data entry to eliminate duplicate entry. Shall auto-populate data fields when possible.
4. Shall have dynamic navigation; in which any window is accessible from any other window. Shall not require the user to leave the flowsheet in order to view other information such as access pictures, problem lists, and essential clinical information.
5. Shall have a physician rounding screen that displays all relevant clinical data on a single screen.
6. Shall have the ability to print screens and reports in the dialysis EHR solution. Shall automatically format data for printing (i.e. lab report, hemodialysis flowsheet).

5.1.8 CROWNWEB INTERFACE

1. The dialysis EHR solution shall be capable of interfacing directly with CROWNWeb and via the NRAA HIE. Costs associated with the CROWNWeb and/or NRAA HIE interface (with the exception of NRAA membership) shall be included in the dialysis EHR solution cost and shall not be reimbursed separately.
2. The dialysis EHR solution shall be capable of automatically capturing all CROWNWeb required data from the appropriate source (such as VistA, user input.); collating data; and directly reporting data to CROWNWeb. CMS requires data to be

- submitted in Extensible Markup Language (XML) format. The dialysis EHR solution shall adhere to current CROWNWeb reporting requirements, business rules, kidney data definitions, and reporting schedules. Refer to Section 2.0 Applicable Documents. The dialysis EHR solution shall transmit data to CROWNWeb according to VA's required mode of secure transmission.
3. The Contractor shall provide all software and associated hardware necessary for the interface between the dialysis EHR solution and CROWNWeb. The cost of the hardware and software necessary for the direct connection to CROWNWeb shall be included in the cost of the dialysis EHR solution and shall not be priced separately.
 4. The dialysis EHR solution shall be capable of reporting to CROWNWeb using the NRAA HIE. The dialysis EHR solution shall maintain NRAA HIE certification throughout the duration of this contract and shall adhere to current NRAA HIE requirements. Refer to Section 2.0 Applicable Documents. Note: VA will be responsible for contracting with NRAA and associated membership.
 5. The Contractor shall provide all software and associated hardware (such as the NRAA Activator application) necessary for the interface between the dialysis EHR solution and the NRAA HIE. The cost of the hardware and software necessary for connection to the NRAA HIE shall be included in the cost of the dialysis EHR solution and shall not be priced separately.

5.1.9 PRINTER INTERFACE

The dialysis EHR solution shall be capable of interfacing directly with non-network (i.e. directly connected to workstation) printers. The cost of this interface shall not be priced separately.

5.2 INSTALLATION AND TESTING

5.2.1 INSTALLATION

The Contractor shall commence installation, implementation, configuration, and testing of the dialysis EHR solution at each facility specified in the individual TO no later than five days after delivery of the dialysis EHR solution. The contractor shall complete installation, implementation, configuration, and testing of the dialysis EHR solution at each facility specified in the individual TO no later than 30 days after delivery unless otherwise agreed to by VA and the contractor. The Contractor shall provide full-service installation of the dialysis EHR solution and all associated interfaces, software, and hardware, including, but not limited to, servers and Ethernet converters. In collaboration with Government personnel determined in the individual task orders, the Contractor shall physically install and set-up all required system components and interfaces and confirm server configurations. Installation shall be performed on-site at the VA facility specified in the individual TO. Within 24 hours of completion of installation, the Contractor shall provide an Installation Report that describes all components installed; all activities associated with the installation, and all stakeholders involved with the installation. Installation service includes all labor, supplies, supervision, travel, per diem, and customary charges required to complete installation. These items shall not be billed separately.

Deliverable:

- A. Installation Report

5.2.2 CONTRACTOR TESTING

Upon completing installation, the Contractor shall test the entire system to ensure proper operation including interfaces with the dialysis machines, Vista, CROWNWeb, and the NRAA HIE. Upon completion of Contractor testing, the dialysis EHR solution and all interfaces shall

be fully functional and the Contractor shall confirm in writing to designated Government personnel that the dialysis EHR solution works as intended; including capture of all data elements from all sources and that the dialysis EHR solution is ready for Government Acceptance Testing (GAT). Submission of System Readiness Notification shall be accomplished by the Contractor prior to initiation of GAT defined below. These items shall not be billed separately.

Deliverable:

A. System Readiness Notification

5.2.3 GOVERNMENT ACCEPTANCE TESTING

The dialysis EHR solution will be tested by the Government (OI&T, biomedical engineering, and clinical staff) to ensure the Government requirements are met. The Contractor shall be available on-site to answer questions during GAT. The dialysis EHR solution shall pass GAT once the Government determines that dialysis EHR solution meets the requirements in this PWS. The Contractor shall provide a test plan and test cases.

Deliverable:

A. Test Plan and Test Cases

5.3 TRAINING

The Contractor shall provide on-site training, on-site go live support, remote training, on-site refresher training, and reference materials at each VA facility specified in the individual task orders.

5.3.1 ON-SITE TRAINING

The Contractor shall contact the Government to schedule training and implementation. Training dates and times shall be coordinated with Government POCs identified in individual task orders. The Contractor shall provide the following on-site training:

1. End-user training: Shall occur no later than five business days after completion of GAT. Shall be a minimum of five days (8 hours per day). Shall be classroom-based and include exercises and shadow optimization training in the dialysis unit. Classroom sessions shall be targeted for specific disciplines (i.e. physicians, nurses, patient care technicians). Training shall include but not be limited to: on-site orientation and training in operation and care of the dialysis EHR solution; demonstration of the dialysis EHR solution and its interface with the dialysis machines, VistA, CROWNWeb, and the NRAA HIE; and actions to be undertaken in the event of failure. The total number of personnel to be trained will be provided to the Contractor (estimate ten trainees per facility).
2. Super user/administrator training: Shall be a minimum of two days (8 hours per day). May be offered as specialized sessions during initial end-user training. Training shall be at the system manager level. Training shall provide users with an understanding of the administrative/managerial/user configuration aspects of the dialysis EHR solution and shall enable super users to educate other staff on use of the system.
3. Biomedical training: Shall be a minimum of three days (8 hours per day). Shall result in comprehensive understanding of the dialysis EHR solution and its associated interfaces and the demonstrated ability to maintain and restore the system to optimum performance when issues occur. Shall include but not be limited to: normal system

maintenance; problem solving; triaging system components to determine the nature of the failure; system monitoring; back-up procedures; recommended corrective actions; and disaster recovery. Training shall depict data flow (source of data, how it's acquired into the dialysis EHR solution, where it's stored, how/when it's replicated) specific to facility implementation.

4. Go-live support: Shall immediately follow initial user training and shall be a minimum of five days. A train-the-trainer concept does not meet this requirement. During go-live support, Contractor staff shall be on-site to assist users and adjust the dialysis EHR solution features as needed to ensure optimal functioning.
5. On-site refresher user training may be requested by a facility for an additional cost per day.

5.3.2 REMOTE TRAINING

The Contractor shall offer web-based training on system installation, configuration, use, and troubleshooting. Web-based training shall be accessible to all users at any time. The web-based training shall include live and recorded webinars, virtual learning environments that provide hands-on training, and recorded product demonstrations.

5.3.3 REFERENCE MATERIALS

The Contractor shall provide hard copies of the Training Materials to each training attendee. Upon completion of installation, the Contractor shall provide each facility specified in the individual task orders with one hard copy of the dialysis EHR User Guide, Installation Guide including installation guides for all interfaces, Administrator Guide, Quick Reference Tip Sheet, and Maintenance/Technical Manuals. All reference materials shall also be provided online and accessible to all users in electronic format (i.e. PDF). The reference materials shall be customized for the VA user as needed.

Deliverables:

- A. Training Materials
- B. EHR User Guide
- C. Installation Guide
- D. Administrator Guide
- E. Quick Reference Tip Sheet
- F. Maintenance/Technical Manuals

5.4 MAINTENANCE AND TECHNICAL SUPPORT

The Contractor shall ensure that the dialysis EHR solution and interfaces are operable and available for use 99.9% of the time, 24 hours a day, seven days a week. The Contractor shall provide scheduled and unscheduled maintenance and technical support for the dialysis EHR solution and associated interfaces throughout the duration of this contract. Contractor-provided hardware shall include a standard commercial warranty that shall be managed by VA and manufacturer supplied maintenance documentation. The Contractor shall provide, perpetual licensed software including all version changes, upgrades, updates, patches, enhancements, corrections, and new releases on a quarterly, or as needed basis. The Contractor shall ensure that all dialysis EHR solution interfaces (such as VistA, dialysis machines, CROWNWeb, NRAA HIE, and printers) and data transfer links are maintained consistently throughout the Period of Performance (PoP). The Contractor shall coordinate with other vendors when necessary to accomplish this task.

Upon completion of any software repairs, updates, and upgrades, the Contractor shall test the system to ensure it is fully functional and in accordance with manufacturer specifications and the requirements in this PWS. The Contractor shall provide each facility specified in the individual task orders with an electronic copy (i.e. PDF) and one hard copy of User Manuals, System Administrator Manuals, Operating/Maintenance and/or Technical Manuals, Release Notes, and Service Bulletins necessary for operation and support of the software and hardware. These documents shall also be available online.

The Contractor shall coordinate maintenance with the local Government personnel. The Contractor shall perform maintenance on-site or remotely. Remote maintenance shall be performed using Contractor equipment. When performing remote maintenance, the Contractor shall comply with VA remote access requirements. Maintenance includes all labor, supplies, parts, and shipping. The Contractor shall provide all tools, test equipment, service manuals, and service diagnostic software necessary to perform any services defined in this PWS.

Deliverables:

- A. User Manuals
- B. System Administrator Manuals
- C. Operating/Maintenance/Technical Manuals
- D. Release Notes
- E. Service Bulletins

5.4.1 TELEPHONE, ONLINE SUPPORT, TECHNICAL CONSULTATION

The Contractor shall provide telephone and online support for routine maintenance and technical assistance, Monday through Friday, 8 a.m. to 7 p.m. Eastern Time. The Contractor shall provide on-call telephone support 24 hours per day, seven days per week, 365 days per year for emergency issues. Contractor support personnel shall be capable of resolving technical issues. The Contractor shall provide a toll-free telephone number and email address to be used by VA for telephone and online support. The Contractor shall provide an online website for field service requests from VA. The Contractor shall allow an unlimited number of requests.

5.4.2 EVENT RESPONSE TIME

All maintenance and technical support services shall be provided in accordance with Table 1. Urgent requests shall be addressed anytime 24 hours a day, seven days a week, 365 days a year. If the problem cannot be resolved over the phone or facilitated remotely, the Contractor shall provide an authorized representative of the company to commence work (on-site physical response) in accordance with the response times listed in Table 1 and shall proceed progressively to rectify the problem without undue delay. The Contractor shall coordinate the method of response with local Government personnel.

Table 1 lists response time requirements by priority type. A priority type is based on impact and urgency and is used to identify required times for actions to be taken by a Contractor. The assignment of a priority type by local Government personnel determines how the incident is to be addressed by the Contractor.

1. **Urgent priority** is defined as any issue that affects life and/or property. Urgent priority applies when malfunction or failure can result in patient injury or death or significant damage to equipment. This includes any issue that adversely impacts patient care. Examples include partial or complete system outages, interruptions making a critical

functionality inaccessible, interruptions causing a severe impact on application availability, or data corruption resulting in missing or incorrect patient information, duplicate records, and loss of data. Urgent priority requires immediate action by the Contractor.

2. **High priority** is defined as having a potential to affect patient care such as degradation in performance or functionality, and work flow interruptions or delays. High priority warrants special attention to take precedence over normal and low priorities. Examples include interruption of critical functionality, access denied to data and systems, sustained degraded or unusable capabilities, not life threatening but having a potential for impact on services availability if not resolved. High priority requires immediate action by the Contractor in order to minimize risk of becoming an urgent priority event.
3. **Normal priority** is defined as a defect or fault event but the system is operable with no impact to patient care. Normal priority requires same day initial action but resolution may take more time. Examples include impairment of non-critical functions or procedures, capabilities that have become unusable or hard to use but with no direct impact on patient care services or system availability. Normal priorities typically have a workaround available. Normal priorities take precedence over low priorities.
4. **Low priority** is defined as preventive maintenance or issues that do not require immediate action or attention.

The Contractor shall meet the following response time requirements associated with each priority. The Contractor shall submit requests to extend the turnaround time to restore the system to full performance to the CO for approval. Full performance means that all defective parts or software have been replaced and that replacement meets or exceeds the required functionality.

Table 1: Response Times (upon receipt of notification from facility point of contact (POC))

Priority	Call Back Response	Remote Log-In Response	Turn Around Time (to restore to full performance)
Urgent	1 hour	1 hour	48 hours
High	2 hours	2 hours	48 hours
Normal	2 hours	8 hours	60 hours
Low	4 hours	10 hours	60 hours

5.4.3 UNSCHEDULED MAINTENANCE

The Contractor shall repair, when requested by local Government personnel, the dialysis EHR solution and restore the dialysis EHR solution to full functionality.

For technical problems, functional incidents, or for questions during business hours, the Contractor shall provide the following communication options for VA: call the Contractor Help Desk, create a field service request online, or email regarding the incident or question.

The Contractor shall communicate the following via email to designated Government personnel in response to each event communicated by VA to the Contractor:

1. Brief description of the problem

2. What version or software package is being affected
3. If this issue affects patient safety
4. Workaround (if any) and expected release date of patch, upgrade, or update (if any)
5. Status and estimated completion date/time

The Contractor shall communicate all known software issues to designated Government personnel including the national CO and COR weekly via email. The Contractor shall respond to a request for unscheduled corrective maintenance for software or failure in accordance with response time requirements defined in Table 1 of Section 5.4.2 Event Response Time.

5.4.4 SCHEDULED MAINTENANCE

The Contractor shall perform scheduled maintenance, including an annual preventative maintenance inspection, of the dialysis EHR solution. The Contractor shall initiate corrective maintenance whenever defects are discovered as a result of the Contractor performing scheduled/preventative maintenance services.

The Contractor shall recommend to designated Government personnel when software should be made available for scheduled maintenance, and upon Government approval, the Contractor shall finalize that schedule. The Contractor shall provide a Scheduled Maintenance Procedures document that includes a description of all tasks, task duration estimates, and the expected frequency of each task type. The Contractor shall provide scheduled maintenance and software updates during normal working hours or at a mutually agreed upon time by the facility POC and the Contractor.

The annual inspection shall be performed within the VA fiscal year third quarter period (April, May, or June). The Contractor shall coordinate and schedule the specific date and time with the facility POC.

Deliverable:

- A. Scheduled Maintenance Procedures

5.4.5 SOFTWARE UPDATES AND UPGRADES

Included in system maintenance is the furnishing and installation of all software upgrades, version changes, and/or updates to the system. The Contractor shall provide software updates and patches, scheduled in advance, in order to keep the software components at the most current software release. The Contractor shall provide any successor versions of the dialysis EHR solution including software updates, version changes, and upgrades at no additional charge to the Government.

The Contractor shall update/upgrade the dialysis EHR solution software, where such update can be 1) initiated by the Contractor to improve functionality; 2) in response to changes in the needs of the VA facility; and 3) to maintain compatibility with other systems as described in Section 5.4.6 Interface Support. The Contractor shall plan and schedule these upgrades with the facility POC. Software updates shall be scheduled five days in advance.

5.4.6 INTERFACE SUPPORT

The Contractor shall ensure that all dialysis EHR solution interfaces (such as VistA, dialysis machines, CROWNWeb, the NRAA HIE, and printers) and data transfer links are maintained consistently throughout the PoP.

5.4.6.1 VISTA INTERFACE

Integration of the dialysis EHR solution with VistA shall be maintained by the Contractor. The Contractor shall be responsible for ensuring that the dialysis EHR solution interfaces with the most recent versions of VistA. When changes to VistA or CPRS occur or new versions are released, the Contractor shall be responsible for ensuring the dialysis EHR solution interface with VistA maintains full functionality.

5.4.6.2 DIALYSIS MACHINE INTERFACE

Integration of the dialysis EHR solution with a facility's dialysis machines shall be maintained and supported by the Contractor. The Contractor shall maintain the dialysis EHR solution's capability of importing physiologic data as a continuous data stream from the dialysis machines. When a VA facility changes, replaces, or upgrades their dialysis machine or machine software, the Contractor shall be responsible for ensuring that the dialysis EHR solution interface with the dialysis machines maintains full functionality.

5.4.6.3 CROWNWEB INTERFACE

The Contractor shall support full integration of the dialysis EHR solution with CROWNWeb. The Contractor shall be responsible for ensuring that the dialysis EHR solution interfaces with the most recent CROWNWeb version and requirements. When changes to CROWNWeb occur, the Contractor shall be responsible for ensuring that the dialysis EHR solution interface with CROWNWeb maintains full functionality.

5.4.6.4 NRAA HIE INTERFACE

The Contractor shall support full integration of the dialysis EHR solution with the NRAA HIE. The Contractor shall be responsible for ensuring that the dialysis EHR solution interfaces with the most recent version of the NRAA HIE. When changes to the NRAA HIE occur, the Contractor shall be responsible for ensuring that the dialysis EHR solution interface with the NRAA HIE maintains full functionality.

5.4.6.5 PRINTER INTERFACE

The Contractor shall support full integration of the dialysis EHR solution with VA workstation printers. The Contractor shall be responsible for ensuring that the dialysis EHR solution interfaces with current VA facility printers. When changes to printers occur, the Contractor shall be responsible for ensuring that the dialysis EHR solution interface with the printer maintains full functionality.

5.5 CONTRACT MANAGEMENT

The Contractor shall provide contract and TO level management. The Contractor shall work closely with the Government to manage contractual and programmatic issues that arise during performance of the contract. The Contractor shall be responsible for the execution of all contract tasks to include, but not be limited to: program reviews; kickoff meetings; status updates; various reporting requirements; and day-to-day concerns.

A national Government CO and COR will address enterprise-wide issues. Ordering VA facilities will designate a facility COR/POC that the Contractor shall work with to coordinate facility orders.

5.5.1 CONTRACT POST AWARD CONFERENCE

The Government intends to convene a Post Award Conference with the awardee within 30 days after contract award. VA will provide a specific date, location, and agenda for the meeting within 10 days after contract award. At the conference, the Contractor shall present the details of the intended approach for managing the contract, including an Initial Draft Contract Level Work Plan and Schedule. All the key Contractor personnel shall be present for this initial review. The Contractor shall provide an Initial Draft Contract Level Work Plan and Schedule, Post Award Conference Meeting Minutes, and an Action Item Summary electronically to the VA COR and all meeting participants no later than 10 days after conclusion of the Contract Post Award Conference.

Deliverables:

- A. Initial Draft Contract Level Work Plan and Schedule
- B. Post Award Conference Meeting Minutes
- C. Action Item Summary

5.5.2 TASK ORDER KICKOFF MEETINGS

If required by the ordering facility, the Contractor shall participate in a TO level kickoff meeting and brief the Government on how it intends to meet the requirements of the TO. The kickoff meeting shall be held via conference call. Specific requirements will be detailed in the individual task orders.

5.5.3 REPORTING REQUIREMENTS

5.5.3.1 QUARTERLY SUMMARY REPORT

The Contractor shall provide, via email, the national COR and CO with Quarterly Summary Reports in Microsoft Office format. The Summary Reports shall cover all task orders issued and completed during the reporting period and task orders planned, to the extent known, for the subsequent reporting period. The report shall track the cumulative contract ceiling. The Summary Report shall identify current implementation status, any problems that have arisen, and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation including its plan and timeframe for resolving the issue. It is expected that the Contractor will maintain timely communication with VA so that issues that arise are transparent to both parties to prevent escalation of outstanding issues. The Summary Reports shall include:

1. Contract/Order Number
2. Date of Award
3. Facility COR/POC Name, Telephone Number, Location
4. Integrated Funds Distribution Control Point Activity Accounting & Procurement (IFCAP) Purchase Order Number
5. Total Dollars Obligated
6. VA Delivery Facility Code (if applicable)
7. VA Delivery Facility Mailing Address (if applicable)
8. Software Version Number, License Type, and Term
9. Maintenance Start Date, End Date, Software Location for each product on the Task Order
10. Technical Support Toll Free Telephone Number and Website

Deliverable:

A. Quarterly Summary Report

5.5.3.2 FIELD SERVICE REPORTS

The Contractor shall provide a Field Service Report (FSR) to the facility POC upon completion of a service call prior to departing the VA facility or at the conclusion of remote service. The Contractor shall obtain the signature or initials of the designated employee on the FSR. For remote service, the FSR shall be managed (sent, received, signed, scanned, returned) electronically. The FSR shall document the services rendered and include a description of the software/equipment serviced, model, barcode/serial number, date and time of service, description of services, the latest version of software patch or upgrade, downtime duration and reason, results of service, name of individual who performed the service, and travel, labor, and parts information. FSR reports shall be summarized in the Quarterly Summary Report described in 5.5.3.1

Deliverable:

A. Field Service Report

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

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

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are PIV-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), http://www.ea.oit.va.gov/VA_EA/VAEA_TechnicalArchitecture.asp, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/enterprise_dp.asp. The Contractor shall ensure all Contractor delivered applications and systems are compliant with VA Identity Management Policy (VAIQ# 7011145), Continued Implementation of Homeland Security Presidential Directive 12 (VAIQ#7100147), and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document), located at <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>. The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63, VA Handbook 6500 Appendix F, "VA System Security Controls", and VA IAM enterprise requirements for direct, assertion based authentication, and/or trust based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of Personal Identity Verification (PIV) and/or Common Access Card (CAC), as determined by the business need. Assertion based authentication must include a SAML implementation. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST 800-63 guidelines. Trust based authentication must include authentication/account binding based on trusted HTTP headers. The

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

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

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

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 11 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Office 2013 and Windows 8.1. However, Office 2013 and Windows 8.1 are not the VA standard yet and are currently not approved for use on the VA Network, but are in-process for future approval by OI&T. Upon the release approval of Office 2013 and Windows 8.1 individually as the VA standard, Office 2013 and Windows 8.1 will supersede Office 2010 and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be delivered as a signed .msi package and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA's current desktop application deployment tool. Signing of the software code shall be through a vendor provided certificate that is trusted by the VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) specific to the particular client operating system being used.

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

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

6.2 SECURITY AND PRIVACY REQUIREMENTS

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

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

Position Sensitivity	Background Investigation (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A)
Low / Tier 1	Tier 1 / National Agency Check with Written Inquiries (NACI) A Tier 1/NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), 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 Risk positions.
Moderate / Tier 2	Tier 2 / Moderate Background Investigation (MBI) A Tier 2/MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree.
High / Tier 4	Tier 4 / Background Investigation (BI) A Tier 4/BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree.

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

Position Sensitivity and Background Investigation Requirements by Task

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

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

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

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

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

Deliverable:

- A. Contractor Staff Roster

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: MS Word 2000/2003/2007/2010, MS Excel 2000/2003/2007/2010, MS PowerPoint 2000/2003/2007/2010, MS Project 2000/2003/2007/2010, MS Access 2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

6.4 PERFORMANCE METRICS

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

[illegible]

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

6.5 FACILITY/RESOURCE PROVISIONS

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

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

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

This remote access may provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath, Primavera, and Remedy, including appropriate seat management and user licenses, depending upon the level of access granted. The Contractor shall utilize government-provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort. The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with VA Handbook 6500, local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. The Contractor shall ensure all work is performed in countries deemed not to pose a significant security risk. For detailed Security and Privacy Requirements (additional requirements of the contract consolidated into an addendum for easy reference) refer to ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED and ADDENDUM B - VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE.

6.6 GOVERNMENT FURNISHED PROPERTY

Not applicable

6.7 SHIPMENT OF HARDWARE OR EQUIPMENT

The Contractor shall complete the Master Delivery Schedule in accordance with the Instructions, and shall coordinate with the COR for specifics. The Master Delivery Schedule shall be provided after award and updated prior to and after each delivery timeframe.

Shipment/Delivery Kick-off Meeting

The Contractor shall conduct a Shipment/Delivery Kick-off Meeting with the VA PM, COR, Delivery Date Coordinator, Implementation Manager, and Facility CIOs (or designee) to discuss delivery schedule requirements and facilitate delivery of equipment. This meeting may be held in conjunction with the post award conference or identified technical kickoff meeting. The Contractor shall also present the Shipment/Delivery Weekly Progress Report format for review and approval by the Government. This meeting, if held independently, shall be conducted telephonically within ten days after award and shall incorporate any delivery schedule changes to the draft Delivery Schedule identified by the Government.

Shipment/Delivery Weekly Progress Report

The Contractor shall provide a Shipment/Delivery Weekly Progress Report which shall identify the items shipped, the serial number associated with each piece of equipment; the date of each shipment; the status of each shipment, tracking information, and information relative to Government-receipt of the equipment items at each delivery site. In addition, the Shipment/Delivery Weekly Progress Report shall identify any problems and provide a description of how the problems were resolved/addressed. If problems have not been completely resolved, the Contractor shall provide an explanation and status of resolution. Shipment/Delivery Weekly Progress Reports shall be submitted in Microsoft Excel Format and shall clearly identify each serial number of the equipment being delivered with one (1) serial number per cell.

Inspection: Destination

Acceptance: Destination

Free on Board (FOB): Destination

Packing Slips/Labels and Lists shall also include the following:

IFCAP PO #: _____ (e.g., 166-E11234 (the IFCAP PO number is located in block #20 of the SF 1449))

Project Description: (e.g. Tier 1 Lifecycle Refresh)

Total number of Containers: Package ____ of _____. (e.g., Package 1 of 3)

Deliverables:

- A. Master Delivery Schedule
- B. Shipment/Delivery Weekly Progress Report

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

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

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

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

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

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

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

A2.0 VA Enterprise Architecture Compliance

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

A2.1. *VA Internet and Intranet Standards*

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

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

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

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

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

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

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

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

A3.2. Equivalent Facilitation

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

A3.3. Compatibility with Assistive Technology

The Section 508 standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device. Section 508 requires that the EIT be compatible with such software and devices so that EIT can be accessible to and usable by

individuals using assistive technology, including but not limited to screen readers, screen magnifiers, and speech recognition software.

A3.4. Acceptance and Acceptance Testing

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

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

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

Deliverables:

- A. Final Section 508 Compliance Test Results

A4.0 Physical Security & Safety Requirements:

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

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

A5.0 Confidentiality and Non-Disclosure

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

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

the Privacy and Security Rules, the Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA CO will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA CO for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA CO.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
 - a. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
 - b. Controlled access to system and security software and documentation.
 - c. Recording, monitoring, and control of passwords and privileges.
 - d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.

- e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
- f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
- g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
- h. Contractor does not require access to classified data.
8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
9. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

A6.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

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

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

1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (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. ***The acquisition of Silver or Gold EPEAT registered products is encouraged over Bronze EPEAT registered products.*** EPEAT registered products are required to meet the technical

specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified product lists. The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists.

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

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

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

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

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

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

B1. GENERAL

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

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

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

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

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

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

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

B3. VA INFORMATION CUSTODIAL LANGUAGE

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

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

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

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

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

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

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

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

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

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

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

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or a Memorandum of Understanding-Interconnection Service Agreement (MOU-ISA) for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

1. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference 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 without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and

c. Include this Privacy Act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR.

8. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the

officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the Contractor/Subcontractor is considered to be an employee of the agency.

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

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

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

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

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

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

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine

vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must be in accordance with the TIC Reference Architecture and reviewed and approved by VA prior to implementation.

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

c. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization) (C&A) of the Contractor's systems in accordance with VA Handbook 6500.3, *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.

d. The Contractor/Subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA 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 subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/Subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

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

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

g. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the Contractor/Subcontractor or any person acting on behalf of the Contractor/Subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the Contractors/Subcontractors that contain VA information must be returned to VA for sanitization or destruction or the Contractor/Subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

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

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

B6. SECURITY INCIDENT INVESTIGATION

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

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

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

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

B7. LIQUIDATED DAMAGES FOR DATA BREACH

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

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

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

- 1) Nature of the event (loss, theft, unauthorized access);
- 2) Description of the event, including:
 - a) date of occurrence;
 - b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
- 3) Number of individuals affected or potentially affected;
- 4) Names of individuals or groups affected or potentially affected;
- 5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
- 6) Amount of time the data has been out of VA control;
- 7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
- 8) Known misuses of data containing sensitive personal information, if any;
- 9) Assessment of the potential harm to the affected individuals;
- 10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Breaches Involving Sensitive Personal Information*, as appropriate; and
- 11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

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

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

B8. SECURITY CONTROLS COMPLIANCE TESTING

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.

B9. TRAINING

- a. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

1) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* course (TMS #10176) and complete this required privacy and security training annually; Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems. Approximate time to complete training is one hour.

2) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access *[to be defined by the VA program official and provided to the CO for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]*

- b. The Contractor shall provide to the CO and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.
- c. Failure to complete the mandatory annual training and electronically sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

ADDENDUM C – LOCATIONS OF VA FACILITIES CURRENTLY PROVIDING DIALYSIS

#	City	State	Service Provided
1	Birmingham	AL	Inpatient, Outpatient
2	Fayetteville	AR	Inpatient
3	Little Rock	AR	Inpatient, Outpatient, Home
4	Phoenix	AZ	Inpatient
5	Tucson	AZ	Inpatient, Outpatient
6	Fresno	CA	Inpatient
7	Mather	CA	Inpatient
8	Loma Linda	CA	Inpatient, Outpatient, Home
9	Long Beach	CA	Inpatient and Outpatient
10	Los Angeles	CA	Inpatient and Outpatient
11	Palo Alto	CA	Inpatient, Outpatient, Home
12	San Diego	CA	Inpatient, Outpatient, Home
13	San Francisco	CA	Inpatient, Outpatient, Home
14	Travis Airforce Base	CA	Inpatient, Outpatient
15	Denver	CO	Inpatient, Outpatient
16	West Haven	CT	Inpatient, Outpatient, Home
17	Washington	DC	Inpatient, Outpatient, Home
18	Wilmington	DE	Inpatient, Outpatient
19	Bay Pines	FL	Inpatient, Outpatient
20	Gainesville	FL	Inpatient, Outpatient
21	Miami	FL	Inpatient, Outpatient
22	Tampa	FL	Inpatient, Outpatient, Home
23	West Palm Beach	FL	Inpatient, Outpatient
24	Augusta	GA	Inpatient
25	Decatur	GA	Inpatient, Outpatient
26	Honolulu	HI	Inpatient, Outpatient
27	Des Moines	IA	Inpatient
28	Iowa City	IA	Inpatient, Outpatient
29	Boise	ID	Inpatient
30	Chicago	IL	Inpatient, Outpatient
31	Hines	IL	Inpatient, Outpatient, Home
32	Marion	IL	Inpatient
33	North Chicago	IL	Inpatient
34	Indianapolis	IN	Inpatient, Outpatient
35	Wichita	KS	Inpatient
36	Lexington	KY	Inpatient, Outpatient
37	Louisville	KY	Inpatient
38	Shreveport	LA	Inpatient
39	Jamaica Plain	MA	Outpatient
40	West Roxbury	MA	Inpatient

41	Baltimore	MD	Inpatient
42	Augusta	ME	Inpatient, Outpatient
43	Ann Arbor	MI	Inpatient, Outpatient
44	Detroit	MI	Inpatient, Outpatient, Home
45	Minneapolis	MN	Inpatient, Outpatient, Home
46	Columbia	MO	Inpatient
47	Kansas City	MO	Inpatient, Outpatient, Home
48	St. Louis	MO	Inpatient, Outpatient, Home
49	Biloxi	MS	Inpatient
50	Jackson	MS	Inpatient, Outpatient
51	Asheville	NC	Inpatient
52	Durham	NC	Inpatient, Outpatient, Home
53	Fayetteville	NC	Outpatient
54	Raleigh	NC	Outpatient
55	Salisbury	NC	Inpatient
56	Fargo	ND	Inpatient
57	Omaha	NE	Inpatient, Outpatient
58	East Orange	NJ	Inpatient, Outpatient
59	Albuquerque	NM	Inpatient, Outpatient, Home
60	N. Las Vegas	NV	Inpatient, Outpatient
61	Reno	NV	Inpatient
62	Albany	NY	Inpatient, Outpatient
63	Bronx	NY	Inpatient, Outpatient, Home
64	Brooklyn	NY	Inpatient, Outpatient, Home
65	Buffalo	NY	Inpatient, Outpatient, Home
66	New York	NY	Inpatient, Outpatient, Home
67	Northport	NY	Inpatient, Outpatient
68	Syracuse	NY	Inpatient
69	Cleveland	OH	Inpatient, Outpatient, Home
70	Cleveland	OH	Outpatient
71	Cincinnati	OH	Inpatient, Outpatient
72	Dayton	OH	Inpatient, Outpatient, Home
73	Muskogee	OK	Inpatient
74	Oklahoma City	OK	Inpatient
75	Portland	OR	Inpatient, Outpatient
76	Lebanon	PA	Inpatient
77	Philadelphia	PA	Inpatient
78	Philadelphia	PA	Outpatient
79	Pittsburgh	PA	Inpatient, Outpatient, Home
80	Wilkes-Barre	PA	Inpatient, Outpatient
81	San Juan	PR	Inpatient, Outpatient
82	Providence	RI	Inpatient, Outpatient
83	Charleston	SC	Inpatient, Outpatient
84	Columbia	SC	Inpatient, Outpatient

85	Hot Springs	SD	Outpatient
86	Sioux Falls	SD	Inpatient
87	Memphis	TN	Inpatient, Outpatient, Home
88	Mountain Home	TN	Inpatient
89	Nashville	TN	Inpatient, Outpatient
90	Amarillo	TX	Inpatient
91	Dallas	TX	Inpatient, Outpatient, Home
92	Houston	TX	Inpatient
93	San Antonio	TX	Inpatient, Outpatient
94	Temple	TX	Inpatient
95	Salt Lake City	UT	Inpatient, Outpatient
96	Hampton	VA	Inpatient, Outpatient, Home
97	Richmond	VA	Inpatient, Outpatient, Home
98	Salem	VA	Inpatient, Outpatient, Home
99	White River Junction	VT	Inpatient
100	Seattle	WA	Inpatient, Outpatient, Home
101	Green Bay	WI	Outpatient
102	Madison	WI	Inpatient
103	Milwaukee	WI	Inpatient, Outpatient
104	Beckley	WV	Inpatient
105	Clarksburg	WV	Inpatient
106	Huntington	WV	Inpatient

SECTION C – CONTINUATION OF SF30 BLOCKS

C.6 52.216-22 INDEFINITE QUANTITY (OCT 1995)

(a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum." The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum."

(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; *provided*, the Contractor shall not be required to make any deliveries under this contract 24-12 months after the expiration of the contract's effective period.

(End of Clause)

C.8 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of the task order by written notice to the Contractor prior to expiration of the contract; provided that the Government gives the Contractor a preliminary written notice of its intent to extend prior to individual task order expiration. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended task order shall be considered to include this option clause.

(c) ~~The Contractor shall not be required to make any deliveries under this contract 24 months after the expiration of the contract's effective period. The total duration of this contract, including the exercise of any options under this clause, shall not exceed 72 months.~~

(End of Clause)