PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS

VA Eastern Colorado Health Care System

LV36 – Vital Signs Monitors

Date: *September 5, 2017*
PWS Version Number: v*2.0*

Contents

1.0 BACKGROUND

This acquisition is in support of the initial outfitting and activation of the new Denver VA Medical Center being constructed in Aurora, CO.

The Veteran Affairs Eastern Colorado Health Care System (VA ECHCS), Denver, CO., requires vital signs monitors with NIBP, temperature, SPO2 with mobile cart, and storage basket. The monitors will be used primarily for outpatient use throughout the campus and shall be integrated to VA Vista/CPRS "Vital Light" module via wired and wireless LAN.

2.0 APPLICABLE DOCUMENTS

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

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

20. VA Handbook 6500.2, "Management of Breaches Involving Sensitive Personal Information (SPI)", July 28, 2016
21. VA Handbook 6500.3, "Assessment, Authorization, And Continuous Monitoring Of VA Information Systems," February 3, 2014
22. VA Handbook 6500.5, "Incorporating Security and Privacy in System Development Lifecycle", March 22, 2010
23. VA Handbook 6500.6, "Contract Security," March 12, 2010
24. VA Handbook 6500.8, "Information System Contingency Planning", April 6, 2011
25. OI&T ProPath Process Methodology (Transitioning to Process Asset Library (PAL) (reference process maps at http://www.va.gov/PROPATH/Maps.asp and templates at http://www.va.gov/PROPATH/Templates.asp
26. One-VA Technical Reference Model (TRM) (reference at http://www.va.gov/trm/TRMHomePage.aspx)
27. National Institute Standards and Technology (NIST) Special Publications (SP)
28. VA Directive 6508, "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 15, 2014
29. VA Handbook 6508.1, "Procedures for Privacy Threshold Analysis and Privacy Impact Assessment," July 30, 2015
30. VA Directive 6300, Records and Information Management, February 26, 2009
31. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
32. OMB Memorandum, "Transition to IPv6", September 28, 2010
33. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015
34. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 24, 2014
35. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
36. OMB Memorandum 05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005
37. OMB memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011
38. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
39. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
40. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
41. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
42. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
43. NIST SP 800-157, Guidelines for Derived PIV Credentials, December 2014
44. NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
45. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014

46. VA Memorandum, VAIQ #7100147, Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12), April 29, 2011 (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
47. VA Memorandum, VAIQ # 7011145, VA Identity Management Policy, June 28, 2010 (reference Enterprise Architecture Section, PIV/IAM (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
48. IAM Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, PIV/IAM (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
49. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, Department of Homeland Security, October 1, 2013, https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf
50. OMB Memorandum M-08-05, "Implementation of Trusted Internet Connections (TIC), November 20, 2007
51. OMB Memorandum M-08-23, Securing the Federal Government's Domain Name System Infrastructure, August 22, 2008
52. VA Memorandum, VAIQ #7497987, Compliance – Electronic Product Environmental Assessment Tool (EPEAT) – IT Electronic Equipment, August 11, 2014 (reference Document Libraries, EPEAT/Green Purchasing Section, https://www.voa.va.gov/documentlistpublic.aspx?NodeID=552)
53. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
54. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
55. Executive Order 13693, "Planning for Federal Sustainability in the Next Decade", dated March 19, 2015
56. Executive Order 13221, "Energy-Efficient Standby Power Devices," August 2, 2001
57. VA Directive 0058, "VA Green Purchasing Program", July 19, 2013
58. VA Handbook 0058, "VA Green Purchasing Program", July 19, 2013
59. Office of Information Security (OIS) VAIQ #7424808 Memorandum, "Remote Access", January 15, 2014, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
60. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
61. VA Memorandum, "Implementation of Federal Personal Identity Verification (PIV) Credentials for Federal and Contractor Access to VA IT Systems", (VAIQ# 7614373) July 9, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
62. VA Memorandum "Mandatory Use of PIV Multifactor Authentication to VA Information System" (VAIQ# 7613595), June 30, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
63. VA Memorandum "Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges" (VAIQ# 7613597), June 30, 2015; https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
64. "Veteran Focused Integration Process (VIP) Guide 1.0", December, 2015, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371
65. "VIP Release Process Guide", Version 1.4, May 2016, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4411
66. "POLARIS User Guide", Version 1.2, February 2016, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4412

3.0 SCOPE OF WORK

The Contractor shall provide all the equipment and services required to provide the VA Eastern Colorado Health Care System (VA ECHCS) with vital signs monitors meeting the specifications defined herein. The Contractor shall also provide the professional services, training, and operations and maintenance services detailed in Section 5 to ensure successful installation and configuration of the required equipment.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

Period of Performance (Operations and Maintenance):

Base Period: 12 months from date of award
Option Period One (1): 12 months
Option Period Two (2): 12 months
Option Period Three (3): 12 months
Option Period Four (4): 12 months

Any work at the Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO).

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

Under current definitions, four are set by date:

New Year's Day	January 1
Independence Day	July 4
Veterans Day	November 11
Christmas Day	December 25

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

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

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

4.2 PLACE OF PERFORMANCE

Installation and configuration tasks under this PWS shall be performed in VA facilities located in Aurora, CO. Work may be performed at remote locations with prior concurrence from the Contracting Officer's Representative (COR).

Operations and Maintenance tasks under this PWS for the base and option periods shall be performed at the Contractor's facilities.

4.3 TRAVEL

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

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall provide the following:

VA ECHCS requires vital signs monitors with NIBP, temperature, SPO2, with mobile cart and storage basket for the Denver VAMC Replacement Facility.

The vital signs monitors shall be installed and configured by an authorized Contractor for the materials, software, equipment, services, and supplies. This includes any services required for professional services, hardware, software, and option year warranties for the Denver VAMC Replacement Facility, as described in the specifications contained herein. Any professional services required for hardware, software, option year, and maintenance will be defined in the Contractor's response to the solicitation.

The Contractor shall fill out the Pre-Assessment 6550 form prior to contract award.

Based on the approved deployment work schedule, the Contractor shall provide all labor necessary to install, deploy, and configure the requirements detailed in this PWS.

The Contractor shall receive and place equipment in the designated areas at the Denver VA Replacement Facility.

The Contractor shall unpack and install all equipment in the designated area to be provided by the Government. The Contractor shall dispose of all trash offsite as there are no adequate onsite trash disposal facilities.

5.1 Monitor, Vital Signs NIBP, Temperature, SPO2 with Cart and Basket (JSN: M4116), Quantity: 102

5.1.1 The contractor shall provide 102 vital signs monitors with NIBP, tympanic temperature, and SPO2, with cart and basket.

5.1.2 Basis of Design: Connex 68XEX-B or equal

5.1.3 The Contractor shall include in their pricing the trade in value of existing vital sign monitors (Welch Allyn Spot LVi) for each new vital sign monitor procured through this acquisition.

Salient Characteristics:

5.1.4 Shall be non-invasive and automatically measure systolic and diastolic blood pressure, pulse rate, temperature, and oxygen saturations (SPO2).

5.1.5 Shall display all values on an easy-to-read display and values can be printed.

5.1.6 Shall have programmable alarms and automatic blood pressure cycles.

5.1.7 Shall provide a choice of measurement modalities.

5.1.8 Shall have not less than 400 reading memory.

5.1.9 Shall incorporate Nellcor Pulse Oximetry (SPO2) algorithms.

5.1.10 Shall measure approximate 15 second NIBP and pulse rate.

5.1.11 Shall capture blood pressure averages and customize interval readings.

5.1.12 Shall connect to the electronic medical record program, VISTA.

5.1.13 Shall allow for manual entries for weight, height, respiration rate, and pain levels.

5.1.14 Shall allow for Ear Thermometry and Acoustic Respiratory Monitoring (RRa).

5.1.15 Shall have data recall.

5.1.16 Shall allow continuous operation.

5.1.17 Dimensions shall not exceed 10” (Height) x 11” (Width) x 6” (Diameter)

5.1.18 Shall not exceed a weight of 9.5 pounds.

5.1.19 Shall have an approximate graphic display resolution pixels minimum of 1024 (H) x 600 (V)

5.1.20 Display are shall not exceed 6” (H) x 4” (V)

5.1.21 Shall include protective classifications for all monitor configurations.

5.1.22 Shall have a pixel arrangement of RGB (red, green, blue).

5.1.23 Shall have a minimum of 16 bits per pixel for color depth.

5.1.24 Shall have an output sound pressure of 67dBat 1.0meter.

5.1.25 Shall have alarm and pulse tones.

5.1.26 Shall have a pulse frequency of 150 to 1000 Hz

5.1.27 Shall have effective pulse duration:

- High Priority: 75 – 200 ms
- Medium and Low Priority: 125 – 250 ms

5.1.28 10-20% effective pulse duration.

5.1.29 Shall have the following battery specifications:

- Rating: Six (6) cell: 11.1 V3.80Ah / Nine (9) cell: 10.8V6.75Ah
- Lithium-Ion
- Charging time to full capacity of approximately three (3) hours

5.1.30 Nurse Call connection specification:

- 25V AC or 60V DC maximum at 1A maximum

5.1.31 NIBP Specifications:

- Cuff pressure range meets or exceeds ANSI/AAMI SP10-2002 standards for cuff pressure range.
- Systolic Range: Adults 30 to 260 mmHg
- Diastolic Range: Adults 20 to 220 mmHg
- Cuff Inflation Target: Adults 150 mmHg
- Maximum Target Pressure: Adults 80 mmHg
- Blood pressure determination time typically is 15 seconds with maximum at 150 seconds.
- Blood pressure accuracy meets or exceeds ANSI/AAMI SP10-2002 standards for noninvasive blood pressure accuracy, +/- 5.0% (+/- 3 beats per second).
- Overpressure Cutoff: Adults 300 mHg +/- 15 mmHg
- Capable to program automatic NIPC cycle every five (5) minutes

5.1.32 Ear Thermometry Module Specifications:

- User-selectable unit of measure in Fahrenheit and Celsius
- Temperature range: 80-110 degrees Fahrenheit
- Calibration accuracy: +/- two (2) degrees Fahrenheit

5.1.33 Nellcor SPO2 Specifications:

- Unit of measure in percent
- One (1) to 100% measurement range
- Saturation accuracy (module): +/- digits, 70 to 100%

5.1.34 Pulse Rate Specifications:

- Unit of measure is beats per minute
- Measurement range is 20 to 250 beats per minute
- Accuracy between +/- three (3) digits

5.1.35 Acoustic Respiration Monitor (RRa) Specifications:

- Unit of measure is breaths per minute
- Measures body weight greater than 66 pounds
- Measurement range between zero (0) to 70 breaths per minute
- Accuracy for adults is four (4) to 70 +/- breaths per minute
- Resolution is one (1) breath per minute

5.1.36 The equipment shall meet the following wireless network interface specifications at a minimum:

- Wireless network interface: IEEE 802.11 b/g, 802.11a – FIPS 140-2 certification
- Security/encryption/authentication: WPA2/AES (either EAP or PSK authentication)
- Approximately two (2) seconds per reading
- Protocols: UDP, DHCP, TCP/IP
- Wired Network: 10/100Mbp VA OIT LAN

5.1.37 Accessories shall include (but not limited to):

- Test system for the maintenance and evaluation of vital signs monitors [one (1) each]

- USB Keyboard [one (1) each)
- Cable Management Mobile Stand with Storage Bin
- 2D Barcode Scanner with Coiled USB Cord

5.2 Software and Server System (JSN: M4116.S)

5.2.1 The software system shall support the following actions:

- Monitor communications with central station through a wireless network
- Establish and continuous monitor profile
- Save vital sign measurements
- Intervals monitoring profiles
- Spot check and change profiles
- Conduct profile comparison
- Integrate to VISTA/CPRS (medical electronic patient record) “Vital Light” module
- HL7 Interface Bi-directional
- Shall allow system administrative access via RDP or web-interface through standard VA OIT PC.

5.2.2 Patient Demographic Recognition

- Via Patient ID Card
- Manual input using patient two (2) identification method

5.2.3 Staff Identification

- Via Staff DUZ barcode label
- Manual input of DUZ number

5.2.4 Server Plan:

- The VA prefers the Contractor utilize virtualization machine (VM) technology. The VAMC will provide VM hardware.
- If a physical server is the requirement for the system to function, the Contractor shall provide all server hardware.
- The Contractor shall provide all operating system licenses such as MS Server, MS SQL
- If MS Server and MS SQL are used, they shall be version MS Server 2012 and MS SQL 2012 or later.

5.2.5 Software Licenses: All necessary licenses shall be included

5.2.6 Accessories shall include but are not limited to:

- Test system for the maintenance and evaluation of vital signs monitors [Quantity: two (2)]

5.3 Installation Services

PROJECT ESTIMATE TIME LINE

Phase I	Project Kickoff	Estimated Start Date: Immediately upon contract award • Kickoff Meeting • Workflow Design
Phase II	Hardware Installation and Testing	Immediately upon Phase I completion
Phase III	Verification and Validation	Immediately upon Phase II completion • Workflow Testing • Vista Integration Testing • Pre Go-Live Training
Phase IV	Go Live	Estimated Start Date: June 25, 2018
Phase V	Post Go-Live	Estimated Start Date: Four (4) months following Go-Live • Follow Up Training • Validate and Review Workflow

5.4 PROJECT MANAGEMENT

5.4.1 The Contractor shall draft a Contractor Project Management Plan (CPMP) that lays out the Contractor's approach, timeline, and tools to be used in execution of the contract. The CMPM should take the form of both a narrative and graphic format that displays the schedule, milestones, risks, and resource support. The CPMP shall include the Contractor's plans for managing all subcontractors.

5.4.2 Topic areas to be addressed in the CPMP shall include: Oversight and communications with subcontractors while onsite at VA locations as well as executing the timely distribution and delivery of materials to subcontractor personnel. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified. The initial baseline CPMP shall be concurred upon and updated monthly therafter. The Contractor shall update and maintain the VA Contracting Officer's Representative (COR) approved CPMP throughout the period of performance. The CPMP shall include (but is not limited to):

- Project Schedule to include Milestones, Deliverables, and Critical Path
- Verification and Validation (V&V) Plan
- Training Plan
- Risks Management Plan
- Operations and Maintenance Plan (See Section 5.10 for further details)
- Project Closeout activities/procedures

5.5 REPORTING REQUIREMENTS

5.5.1 The Contractor shall provide weekly progress reports, to include schedule updates, to the VA COR and shall cover all work completed during the reporting period and work planned for the subsequent reporting period. The reports shall also identify any problems that have arose and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation. The Contractor shall monitor performance against the CPMP and report any deviations. It is expected that the Contractor will remain in communication with the VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

5.5.2 The Contractor shall provide the COR with Monthly Installation Progress Reports in electronic format in Microsoft Word, Project format, or PDF. The report shall include detailed instructions/explanations for each required data element to ensure that data is accurate and consistent. These reports shall reflect data as of the last day of the preceding month. These reports shall include a summary of the task order deliverables.

5.6 Verification and Validation Requirement (Testing)

5.6.1 The Contractor shall perform testing following installation to ensure the vital signs monitor systems are correctly interfaced with VISTA (electronic medical records system) through HL7.

5.6.2 The Contractor shall coordinate with VA OI&T to ensure correct and proper wireless connectivity before the Contractor departs the site and before turnover of equipment. VA ECHCS will not accept equipment that is not correctly interfaced.

5.6.3 The Contractor shall provide a final test plan that includes updates addressing any comments provided by the VA to the draft test plan.

5.6.4 The Contractor shall perform all installation and configuration services necessary to complete the work detailed in this PWS in addition to performing technical service checks to ensure the products are fully operational in accordance with the manufacturer's operating standards.

5.6.5 Acceptance testing is to be performed by the Contractor and VA personnel.

5.6.6 Any disputes that arise shall be resolved by the Contracting Officer.

5.6.7 The Contractor shall conduct a joint inspection with the onsite POC upon completion of delivery.

5.6.8 In the event deficiencies are identified, the Contractor shall provide a date when the identified deficiencies will be addressed; if not addressed on the date of delivery.

5.6.9 The Contractor shall conduct a joint inspection with the onsite POC after addressing all deficiencies.

5.6.10 All deficiencies identified during joint inspections shall be corrected by the Contractor before the Government's acceptance of the item.

5.7 Project Phase Requirements

5.7.1 The Contractor shall provide a single point of contact for the implementation of this project.

5.7.2 The Contractor shall be onsite for one (1) business day for the project kickoff meeting with the client and VA engineering staff.

5.7.3 The Contractor shall develop a project plan in accordance with the site Master Schedule so as not to affect any other deployments or the opening of the Denver VA Replacement Facility.

5.7.4 The Contractor shall confirm and communicate the hardware delivery and implementation schedule.

5.7.5 The Contractor shall manage implementation and associated risk.

5.7.6 The Contractor's Senior Supervisor shall be onsite during the equipment/software installation phase.

5.7.7 The Contractor shall schedule startup of all new equipment.

5.7.8 The Contractor's Project Manager shall communicate any issues and notify the appropriate resources for resolution.

5.7.9 The Contractor shall provide an implementation plan and schedule an implementation meeting within two (2) weeks from order shipment. The Contractor shall identify specific deployment tasks and milestones in the implementation plan.

5.7.10 The Contractor shall provide and maintain an accurate, detailed inventory list of the Contractor installed equipment and software including serial numbers, Equipment Entry (EE) tag numbers, version release, and licenses.

5.8 Training Requirement

5.8.1 The Contractor shall provide onsite clinical training at the Denver VA Medical Center for no more than 100 clinicians, in small groups with 30 minute instruction sessions, not to exceed eight (8) hours per day. Training, at a minimum shall include: end user roles/responsibilities,

how to safely operate the product, and safety features. The Contractor shall provide a competency check-off sheet for each individual upon completion of training.

5.8.2 The Contractor shall provide online technical training and certification for the VA ECHCS eight (8) Biomedical Engineering staff. Training, at a minimum, shall include troubleshooting, performing preventative maintenance, and technical support.

5.8.3 The Contractor shall provide a minimum of two (2) days of follow-up end user training and system administrator training six (6) months after Government acceptance.

5.9 Assembly and Installation

5.9.1 The Contractor is required to manage and coordinate the installation timeline at the Denver Replacement Facility with the VA ECHCS Point of Contact.

5.9.2 The Contractor shall assemble, configure, and test the equipment to ensure the vital signs monitors are operating in accordance with manufacturer's standards.

5.9.3 The Contractor shall install their applications onto a Government provided host machine.

5.9.4 The Contractor shall provide an Excel cut sheet of the serial number for each piece of equipment installed listing IP addresses and MAC addresses for all equipment that attaches to the network by IDF.

5.10 Operations and Maintenance

5.10.1 The Contractor shall provide telephone and remote diagnosis and technical support 24 hours a day/seven (7) days a week.

5.10.2 If the issue cannot be resolved through remote access, the Contractor shall provide onsite support.

5.10.3 The Contractor shall provide hardware (if applicable) and software support to include: updates and upgrades; software licenses; and Window Anti-Virus protection.

5.10.4 The Contractor shall provide VISTA interface mapping reconfiguration twice a year, at the most.

5.10.5 Option Period One (1): Operations and Management Services as described in Section 5.10 for the period of 12 months from the date the base period ends.

5.10.6 Option Period Two (2): Operations and Management Services as described in Section 5.10 for the period of 12 months from the date the first option period ends

5.10.7 Option Period Three (3): Operations and Management Services as described in Section 5.10 for the period of 12 months from the date the second option period ends.

5.10.8 Option Period Four (4): Operations and Management Services as described in Section 5.10 for the period of 12 months from the date the third option period ends.

6.0 GENERAL REQUIREMENTS

6.1.1 General Conditions (Delivery)

6.1.1.1 This acquisition is part of the initial outfitting and activation of the new Denver VA Medical Center being constructed in Aurora, CO. Delivery will be coordinated after award of the order. The Contractor shall contact the Technical Onsite Point of Contact (POC) to schedule a pre-

delivery meeting to be conducted approximately 30 days before the initial award delivery date for verification of delivery dates. Technical Onsite POC for this requirement is:

Lauren Hill (W) – (720) 857-5935 (C) – (407) 233-7054
Email: Lhill@MartekGlobal.com

6.1.1.2 The Contractor may be required to adjust the delivery date from the date specified in the purchase order due to situations beyond the Government's control. The Government reserves the right to adjust the delivery date specified in the award for up to 90 days at no additional cost to the Government.

6.1.2 Requirements

6.1.2.1 Onsite assembly and installation of items and performance of the services identified in this SOW will take place during normal business hours that have been identified as: 0700 to 1600 (7:00 a.m. to 4:00 p.m.) Mountain Time; Monday through Friday; excluding Federal Holidays. See section 4.1 of this PWS.

6.1.2.2 Secure storage is limited at the Denver VA Replacement Facility. If secure storage is required, the Contractor shall make arrangements locally at no additional cost to the Government.

6.1.2.3 The Contractor shall provide all tools, labor, and materials to complete assembly and installation of the required equipment detailed in this PWS.

6.1.2.4 The Contractor shall have available an Onsite Representative to serve as the primary interfae with the Denver VA Medical Center and VA ECHCS during the duration of assembly and installation of the required equipment detailed in this PWS.

6.1.2.5 The VA will provide a staging area for the equipment to be staged before deployment.

6.1.2.6 Delivery Location

6.1.2.6.1 The Contractor shall deliver all equipment to:

VA Eastern Colorado Health Care System

PVN Dock
1700 North Wheeling Street
Aurora, CO 80045

6.1.2.7 Delivery Markings

6.1.2.7.1 The Contractor shall deliver items in the Original Equipment Manufacturer (OEM)'s original sealed containers with the OEM's name clearly marked thereon.

6.1.2.7.2 The Contractor shall deliver all items marked with the IFCAP Purchase Order Number (ex: 259C70000) and the Award Document Purchase Order Number (ex: VA701-17-P-0000).

6.1.2.8 Delivery Coordination

6.1.2.8.1 All deliveries shall be coordinated with the Onsite POC identified in section 6.1.1.1. Deliveries that are not properly coordinated will be rejected.

6.1.2.9 Site Delivery Conditions

6.1.2.9.1 There shall be no eating, drinking, or smoking inside the construction site at any time.

6.1.2.9.2 All delivery personnel shall comply with all posted safety requirements to include the wearing of Personal Protection Equipment (PPE). Minimum PPE requirements are: Hard hat, over-the-ankle boots, reflective safety vest, eye protection, and gloves.

6.1.3 Use of Premises

6.1.3.1 Requirements

6.1.3.1.1 During the performance of this contract, all work shall be conducted at the VA Denver Replacement Hospital. The Contractor shall perform all work in a manner that will cause minimal interference with VA ECHCS operations and the operation of other Contractors on the premises.

6.1.3.2 The Contractor shall coordinate and cooperate with VA ECHCS's General Contractor and Construction Manager during delivery and installation activities. All coordination with the General Contractor shall be coordinated through the Technical Onsite POC.

6.1.3.3 The Denver Replacement Facility is currently an active construction site. The Contractor shall assume all responsibility for taking precautions for the Contractor's (and any associated Subcontractors) employees, agents, licensees, and permittees.

6.1.3.4 Prior to commencing work, the Contractor and associated personnel (including Subcontractors) shall be required to attend a VA Construction and Facilities Management Site Safety Training Program.

6.1.3.5 Clean up and disposal: There are no trash disposal facilities or dumpsters available for Contractor use at the Denver VA Replacement Facility for the disposal of material. The Contractor shall clean up all debris and discard at the Contractor's expense.

6.1.3.6 The removal of waste and/or excess material shall be conducted through the loading area. Delivery trucks and/or other Contractor vehicles shall not be permitted to remain in the loading area. Vehicles shall be brought back to the area if required to remove any waste, tool, or excess materials.

6.1.4 Protection of Property

6.1.4.1 Requirements

6.1.4.1.1 The Contractor shall conduct an inspection walk-through of the building(s) and ground with the Technical Onsite POC before commencing any work.

6.1.4.1.2 The Contractor shall protect all items from damage during delivery. The Contractor shall take all precaution to protect against damage to the building(s), grounds, and furnishings. The Contractor shall be responsible for the repair and replacement of any items related to the building(s) and grounds damaged (whether accidentally or on purpose), due to action by the Contractor or their representative.

6.1.4.1.3 The Contractor shall be responsible for repairing and replacing any items, components, building(s), and grounds damaged due to negligence and/or actions taken by the Contractor or its employees or representatives. The source of all repairs beyond simple surface cleaning is the Facility Construction Contractor (or appropriate Subcontractor) so that building warranty is maintained. Concurrence for the VA Facilities Management POC and Technical Onsite POC is required before the Contractor may perform any significant repair work. In all

cases, repairs shall utilize materials of the same quality, size, texture, grade, and color to match adjacent existing work.

6.1.4.1.4 The Contractor shall be responsible for securing all items, their work, tools, and equipment used during delivery and installation.

6.2 ENTERPRISE AND IT FRAMEWORK

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (One-VA TRM). One-VA TRM is one component within the overall 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 set forth in OMB Memoranda M-04-04, M-05-24, M-11-11, as well as the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, and supporting NIST Special Publications. OMB Memoranda M-04-04, M-05-24, and M-11-11 can be found at: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-04.pdf, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-24.pdf, and https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf respectively. The identity authentication Level of Assurance (LOA) requirement for this specific effort is LOA-4.

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directives issued by the Office of Management and Budget (OMB) on August 2, 2005 (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf) and September 28, 2010 (https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf). IPv6 technology, in accordance with the USGv6 Profile (NIST Special Publication (SP) 500-267 (http://www-x.antd.nist.gov/usgv6/index.html), the Technical Infrastructure for USGv6 Adoption (http://www.nist.gov/itl/antd/usgv6.cfm), and the NIST SP 800 series applicable compliance

(http://csrc.nist.gov/publications/PubsSPs.html) shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. In addition to the above requirements, all devices shall support native IPv6 and/or dual stack IPv6 IPv4 connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 and/or dual stack IPv6 IPv4 users and all internal infrastructure and applications shall communicate using native IPv6 and/or dual stack IPv6 IPv4 operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services in dual stack solutions, in addition to OMB/VA memoranda, can be found at: https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282.

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf), M08-23 mandating Domain Name System Security (NSSEC) (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf.

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 (PAL), the OI&T-wide process management tool that assists in the execution of an IT project (including adherence to VIP standards). PAL serves as an authoritative and informative repository of searchable processes, activities or tasks, roles, artifacts, tools and applicable standards or guides to assist project teams in facilitating their VIP compliant work.

6.3 SECURITY AND PRIVACY REQUIREMENTS

There are no additional security and privacy requirements applicable to this requirement.

6.3.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

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

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.4	☒	☐	☐
5.5	☒	☐	☐
5.6	☒	☐	☐
5.7	☒	☐	☐
5.8	☒	☐	☐
5.9	☒	☐	☐

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.

6.3.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
b. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the ProPath (PAL) template. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background

Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.

c. The Contractor should coordinate with the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized. The Contractor shall bring their completed Security and Investigations Center (SIC) Fingerprint request form with them (see paragraph d.4. below) when getting fingerprints taken.

d. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
    1) Optional Form 306
    2) Self-Certification of Continuous Service
    3) VA Form 0710
    4) Completed SIC Fingerprint Request Form

e. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).

f. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via e-QIP).

g. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.

h. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC), completed training delineated in VA Handbook 6500.6 (Appendix C, Section 9), signed "Contractor Rules of Behavior", and with a valid, operational PIV credential for PIV-only logical access to VA's network. A PIV card credential can be issued once your SAC has been favorably adjudicated and your background investigation has been scheduled by OPM. However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of OPM.

i. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.

j. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.
k. Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

6.4 METHOD AND DISTRIBUTION OF DELIVERABLES

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

6.5 PERFORMANCE METRICS

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

Performance Objective	Performance Standard	Acceptable Levels of Performance
A. Technical / Quality of Product or Service	1. Demonstrates understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Provides quality services/products	Satisfactory or higher
B. Project Milestones and Schedule	1. Established milestones and project dates are met 2. Products completed, reviewed, delivered in accordance with the established schedule 3. Notifies customer in advance of potential problems	Satisfactory or higher
C. Cost & Staffing	1. Currency of expertise and staffing levels appropriate 2. Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
D. Management	1. Integration and coordination of all activities to execute effort	Satisfactory or higher

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

6.6 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.

6.7 GOVERNMENT FURNISHED PROPERTY

There is no Government Furnished Equipment (GFE) that will be provided for the completion of this requirement.

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

VA Maintenance/Installation Contracts

**Reference: VA Handbook 6500.6 Appendix C – VA Information and Information System Security/Privacy Language for Inclusion to Contracts, as appropriate*

1. VA INFORMATION CUSTODIAL LANGUAGE

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 the 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. SECURITY INCIDENT INVESTIGATION

The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The contractor/subcontractor shall immediately notify the COTR 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.

3. LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the contractor/subcontractor processes or maintains under this contract.

b. Based on the determinations of the independent risk analysis, the contractor shall be responsible for paying to the 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 $20,00.00 coverage at $0 deductible; and

(6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

4. 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) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix E relating to access to VA information and information systems;

(2) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* training and annually complete required privacy and security training; and

(3) Successfully complete any additional information security or privacy training, as required for VA personnel with equivalent information system access.

b. The contractor shall provide to the contracting officer and/or the COTR 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 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.