PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS
OIT, DSO, SD, TPO - LEC

Request for Information: 36C10B26Q0588
Date: June 26, 2026

PWS Version Number: 1.0

DRAFT

Contents

1.0 BACKGROUND 3
2.0 APPLICABLE DOCUMENTS 3
3.0 SCOPE OF WORK 4
4.0 PERFORMANCE DETAILS 5
4.1 CONTRACT TYPE 5
4.2 PERFORMANCE PERIOD ..... **Error! Bookmark not defined.**
4.3 PLACE OF PERFORMANCE 6
4.4 TRAVEL 6
5.0 SPECIFIC TASKS AND DELIVERABLES 6
5.1 MEETING REQUIREMENTS 6
5.2 RECURRING VOICE AND DATA SERVICES 6
5.3 ESTABLISHMENT OF SERVICES 8
5.4 SERVICE LEVEL AGREEMENT (SLA) 9
5.5 MAINTENANCE PERFORMANCE 10
5.6 ACCOUNT RECORDS AND REPORTING 11
6.0 GENERAL REQUIREMENTS 11
6.1 POSITION/TASK RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS ..... **Error! Bookmark not defined.**
6.2 METHOD AND DISTRIBUTION OF DELIVERABLES ..... **Error! Bookmark not defined.**
6.3 PERFORMANCE METRICS ..... **Error! Bookmark not defined.**
6.4 FACILITY/RESOURCE PROVISIONS 11
6.5 GOVERNMENT FURNISHED INFORMATION .. **Error! Bookmark not defined.**
7.0 ACRONYMS 14

DRAFT

1 BACKGROUND

The Veterans Affairs (VA) Office of Information Technology (OIT), Development Security Operations, Solution Delivery, Telecommunications Provisioning Office (TPO), Local Exchange Carrier (LEC) has the overall business and management responsibilities for all telephone services. The TPO is currently responsible for the management of IT operational expenses for VA Medical Centers (VAMC), Veteran Outreach Centers, Community Based Outpatient Clinics (CBOC) Veterans Benefits and National Cemeteries, and other VA facilities across the Enterprise. The proposed project will allow OIT to centralize management of telephone services and accomplish its goal of reducing overall telecommunications expenses

2 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement (PWS), 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, “Personal Identity Verification of Federal Employees and Contractors,” March 2006
4. 10 U.S.C. § 2224, "Defense Information Assurance Program"
5. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
6. 42 U.S.C. § 2000d “Title VI of the Civil Rights Act of 1964”
7. Department of Veterans Affairs (VA) Directive 0710, “Personnel Suitability and Security Program,” May 18, 2007
8. VA Directive 6102, “Internet/Intranet Services,” July 15, 2008
9. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
10. OMB Circular A-130, “Management of Federal Information Resources,” November 28, 2000
11. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
12. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
13. 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
14. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
15. VA Directive 6500, “Information Security Program,” August 4, 2006
16. VA Handbook 6500, “Information Security Program,” September 18, 2007
17. VA Handbook 6500.1, “Electronic Media Sanitization,” March 22, 2010
18. VA Handbook 6500.2, “Management of Security and Privacy Incidents,” June 17, 2008.

DRAFT

19. VA Handbook 6500.3, “Certification and Accreditation of VA Information Systems,” November 24, 2008.
20. VA Handbook, 6500.5, Incorporating Security and Privacy in System Development Lifecycle.
21. VA Handbook 6500.6, “Contract Security,” March 12, 2010
22. Technical Reference Model (TRM) (reference at http://www.va.gov/trm/)
23. National Institute Standards and Technology (NIST) Special Publications
24. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008
25. VA Directive 6300, Records and Information Management, February 26, 2009
26. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
27. GAO-12-620R GAO's Work Related to the Interim Crosscutting Priority Goals under the GPRA Modernization Act, dated May 31,2012
28. 47 C.F.R. Part 64, Appendix A and B. Wireline telecommunications service priority system for national security and emergency preparedness.

3 SCOPE OF WORK

The Contractor shall provide LEC voice and data communications services at VA locations in Indiana, Kentrucky, Nebraska, New Jersey, New Mexico, and Pennsylvania in accordance with Section 5.2. Voice and data services include but are not limited to: Plain Old Telephone Service (POTS) Line Flat Rate, Primary Rate Integrated (PRI) Services Digital Network (ISDN), Direct Inward Dialing (DID) for each line, and Caller ID on PRI. The VA must be listed and retained as the customer of record. Contractor must own the services/infrastructure being provided.

The long-distance carrier for all voice services must be Qwest Networx Primary inter-LATA Carrier (PIC/LPIC 0432) and frozen to only the specified long-distance carrier. Any identified billing charges or invoicing errors due to vendor's pic/lpic errors shall be the sole responsibility of the vendor to correct.

Contractor shall utilize the VA OB-10 system or an approved Electronic Data Interchange (EDI) software system to electronically submit invoices for processing. Invoices must contain the following items for them to be considered valid for payment:

Current Purchase Order Number	Account Number
Bill Date	Billing Address
Invoice Number	Service Period of Performance (POP) Date
Service Delivery Point Name/Address	Description of Services
Quantity	Unit Price
Total Price	Remittance Address
Remittance POC	Tax ID Number

If invoices do not comply with requirements they will be rejected and not paid. Invoices must be submitted on a monthly basis in arrears. Upon completion of the POP and the

DRAFT

final invoices are paid Contractor must notify the Contracting Officer Representative (COR) and the Contracting Officer (CO) so the purchase order can be closed out.

All disconnect or discontinuations of service requests will stop billing within 30 days of the VA's original requested date to the Contractor regardless of whether or not the Contractor has discontinued the service.

All VA accounts must be identified in their network as a Federal Government account and will not be subject to disconnect for any reason other than the Government requests that it be disconnected.

4 PERFORMANCE DETAILS

4.1 Contract type

This is a Firm-Fixed-Price (FFP) contract.

4.2 Period of Performance

The period of performance for the contract shall be a three-month transition period from date of award, followed by a nine-month base, plus four (4) 12-month option periods. The specific period of performance is listed below:

Transition Period: 12/01/2026 to 02/28/2027
Base Period: 03/01/2027 to 11/30/2027
Option 1: 12/01/2027 to 11/30/2028
Option 2: 12/01/2028 to 11/30/2029
Option 3: 12/01/2029 to 11/30/2030
Option 4: 12/01/2030 to 11/30/2031

Installation, maintenance, and/or disconnection of services shall commence between 8:00 AM to 4:30 PM, Monday through Friday, excluding Federal holidays. Work may be required outside of normal business hours due to system failures and other issues.

There are 11 Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

New Year's Day	January 1
Martin Luther King's Birthday	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Juneteenth National Independence Day	June 19
Independence Day	July 4
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veterans Day	November 11

DRAFT

Christmas Day	December 25
Thanksgiving	Fourth Thursday in November

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.

4.3 Place of performance

Please see Attachment 1 - P02 Market Research Workbook for Service Delivery Points.

4.4 Travel

Contractor travel is not required for this contract.

5 SPECIFIC TASKS AND DELIVERABLES

5.1 Meeting requirements

For successful management and contract surveillance, the following reviews are required.

5.1.1 Program progress reviews

The Contractor shall conduct Program Progress Reviews (PPR) for Government personnel at a mutually agreeable facility (meeting can be virtual). The Contracting Officer (CO)/Contract Specialist (CS) or the Contracting Officer Representative (COR) will schedule the initial PPR. It is anticipated the first PPR will occur no later than 90 calendar days after the date of contract award. Thereafter, PPRs shall occur quarterly, for the life of the contract. During each PPR, the Contractor shall present material that addresses:

1. Status of current services
2. Activities determined to be of importance to VA, such as unanticipated problems
3. Status of significant issues
4. How issues are to be resolved by VA or Contractor

The Contractor shall produce and distribute the PPR meeting minutes identifying the key discussion points and action items. The Contractor shall deliver the PPR meeting minutes to the COR within five business days after the PPR.

5.2 Recurring voice services

The Contractor shall provide LEC telecommunication voice services as listed in section 5.2.1. This is based on services currently in place and where commercially available.

5.2.1 Service types and features

The Contractor shall provide the service types required as listed on the SDP.

DRAFT

5.2.1.1 Service types

5.2.1.1.1 Plain Old Telephone Service (POTS) Line Flat Rate/ePOTS
5.2.1.1.2 Plain Old Telephone Service (POTS) Ground Start Flat Rate/ePOTS
5.2.1.1.3 Primary Rate Integrated Services Digital Network (ISDN) (PRI) service shall be delivered over T-1 format as 23B+D and N1 unless specifically modified under the individual task order PRI (Primary Rate ISDN) service shall be delivered over T-1 format as 23B+D unless specifically modified under the individual order.
5.2.1.1.4 Direct Inward Dialing (DID)/ Direct Outbound Dialing (DOD) Group

5.2.1.2 Service features

5.2.1.2.1 Caller ID feature (POTS Line)
5.2.1.2.2 Three Way Calling feature (POTS Line)
5.2.1.2.3 Call Forward feature (POTS Line)
5.2.1.2.4 Call Forward Busy feature (POTS Line)
5.2.1.2.5 Call Forward No Answer feature (POTS Line)
5.2.1.2.6 Call Waiting feature (POTS Line)
5.2.1.2.7 Voicemail feature (POTS Line)
5.2.1.2.8 Call Block feature (block 411, 900/976) (POTS Line)
5.2.1.2.9 Call Hunting/Roll over feature (POTS Line)
5.2.1.2.10 Third Party Billing Block feature (POTS Line)
5.2.1.2.11 Remote Access to Call Forwarding
5.2.1.2.12 Call Redirect (must include Screening Removal for the Veterans Help line)
5.2.1.2.13 Screening Removal (must include Call Redirect for the Veterans Help line)
5.2.1.2.14 Anonymous Call Reject

5.2.2 Local telecommunication features

Features that are not commercially available must be noted in the response. This may include call forwarding, call waiting, voice mail, conference calling, and call blocking as examples.

5.2.3 Telecommunication availability

The Contractor shall provide telecommunication services 24 hours per day, seven days per week, 365 days per annum. The Contractor shall adhere to all Public Utilities Commission (PUC) Agreements that regulate the area of service. The PUC shall be the primary ombudsman for regulated services. Government LEC services requirements and conditions may be more stringent than PUC regulations and both may apply. All Contractors and their subcontractors must be recognized and regulated by the PUC in the area that the Contractor offers service. Rate and service schedules must comply with both Federal Communications Commission (FCC) and PUC rules. LEC service providers must have their own facilities in the network fully or in part. Best effort service

DRAFT

shall not be accepted. The Government requires telephone service portability and that established telephone numbers be retained.

5.2.4 Telecommunications service priority

The Contractor shall comply with the assignment of a Telecommunications Service Priority (TSP) to all circuits ordered. TSP is a program that authorizes National Security and Emergency Preparedness (NS/EP) organizations to receive priority treatment for vital voice and data circuits or other telecommunications services as a result of hurricanes, floods, earthquakes, and other natural or man-made disasters (see http://tsp.ncs.gov). The TSP Program requires service vendors to prioritize requests by identifying those services critical to NS/EP based on the Federal Communications Commission (FCC) mandate (REF: 88-341). A TSP assignment ensures that it shall receive priority attention by the service vendor before any and all non-TSP service. The Contractor shall ensure that the Department of Veterans Affairs is the customer of record.

5.2.5 E-911 PS/ALI availability

The Contractor shall comply with all applicable local and FCC regulatory requirements including Local Number Portability (LNP), directory assistance, and emergency services (911 or E911) requirements to identify the location of an originating station and route them to the appropriate Public Safety Answering Point (PSAP).

5.3 Establishment of services

The Contractor shall provide telecommunication services that are available 24 hours a day, 7 days a week, 365 days a year (to include all materials, equipment, and labor) for the locations specified in the PWS. Establishment of services includes all non-recurring charges specific to each facility. The Contractor shall seek permission via local Point of Contact (POC) to enter the Government facility for the purpose of installing, inspecting or repairing of the services/equipment, or upon termination of the service, for the purpose of removing Contractor services/equipment.

Requirements for access to VA facilities shall include the following:

1. Normal working hours at VA facilities are 8:00 AM to 4:30 PM except for the Network Operations Center (NOC) which is open 24/7. Overtime or access after normal administrative hours shall be coordinated and approved with each site.
2. Contractor Technicians shall require escorts for in-building work where security requirements dictate; a maximum of four (4) escorts will be provided at each VA location depending on staff availability. The intent is for escorts to be dedicated resources.
3. If work must be conducted after normal working hours, pre-notification must be given to VA Telecom Manager to coordinate VA escorts at a minimum of 48 hours in advance of technician arrival.

DRAFT

5.4 Service level agreement (SLA)

The Contractor services shall conform to SLA parameters as defined in the following subtasks. This SLA shall apply from the Government Acceptance Date for the Service to the duration of the Service Term. Satellite, cellular, or other radio services shall not be an acceptable solution.

5.4.1 Contractor customer support

The Contractor shall provide technical help desk support. Technical help desk support is required 24 hours a day, 7 days a week, and 365 days year. A toll-free number shall be designated as the primary help number for VA to call to report a trouble ticket. Automated answering or ticket automation service shall not be an acceptable solution. The Contractor's customer service representative shall be located in the Continental United States (CONUS) and also be fluent in spoken and written English. A Trouble Ticket is the method used by the Government to advise the Help Desk of a perceived fault, including a Service Outage or a failure to meet an SLA. A unique Trouble Ticket reference number shall be given to the Government representative and also used each time the Government calls in to the Help Desk for any fault update or, if appropriate, to inform the Contractor of restoration of the service.

5.4.2 Mean time to repair (MTTR)

MTTR is the average time for the Contractor to restore the service during a service outage in a billing month. The SLA for MTTR shall be four (4) hours for outage and 72 hours for service degraded. The Contractor shall provide technical support/resolution during established business hours to assist VA with issues pertaining to the LEC Services in Section 5.4.1. MTTR times begin when the Contractor receives a support request from VA. The Contractor shall respond to VA's support requests according to the following fault classifications.

5.4.2.1 Priority 1– service outage

A Service Outage is defined as an unscheduled period in which the service is interrupted and unavailable for use by Customer for 60 or more Unavailable Seconds within a 15-minute period. This includes a business impacting function or service is not available such as loss of dial tone, inability to dial 911, or inability to receive a call on the circuit due to service outages. This shall include total loss of service, or the service is degraded to the extent where the Government is unable to use it. This shall include the inability to receive or transmit data or access critical medical systems due to circuit impairment. The Contractor shall respond to all Service outages within four hours. Notifications shall be provided to VA local POC every business day via telephone until restored. The fault shall not return for seven calendar days, or it shall be considered a continuation of the original service impact.

DRAFT

5.4.2.2 Priority 2– service degraded

Service degraded means VA's workflow is not seriously affected or limited. The Contractor repair technician shall respond to all Service degraded reports within four hours. Status notifications shall be provided to VA local POC every business day via telephone until restored. The fault shall not return for 30 calendar days, or it shall be considered a continuation of the original fault.

5.4.2.3 Exclusions

During scheduled maintenance of the LEC Service, the Contractor shall notify VA within three business days of the maintenance window and describe in detail how long and to what level degraded service is to be expected. The Contractor shall obtain approval in advance from the appropriate VA POC before scheduled maintenance occurs. The voice service shall not be considered to be unavailable for any outage that results from any maintenance performed by the Contractor as defined by the following three exceptions:

1. VA is notified at least three business days in advance of outage or service degradation;
2. During the installation period; or
3. Trouble beyond the demarcation point or Network Interface (NI) not caused by the Contractor.

DRAFT

5.5 Maintenance Performance

The Contractor shall obtain the approval of the VA Facility Telecommunications Manager (TM) prior to starting any work that will cause a service outage (refer to PWS Section 5.4.2.1). The Contractor shall notify the COR and VA Facility TM, if work needs to be performed outside of normal business hours, a minimum of three business days before the work is to begin (except in the case of Trouble Ticket repair). The Contractor shall receive approval from the VA Facility TM prior to commencement of either intrusive testing or contractor actions which may affect service quality.

Service charges for trouble beyond the demarcation point not caused by the Contractor (refer to PWS Section 5.4.2.1) shall be charged to the Government at the rates established by the State PUC. These charges may include a Trouble Isolation Charge (TIC) as well as charges for time or materials for the purpose of reestablishing the service or clearing the fault.

The Contractor shall clean up all work areas immediately after completing work in VA facilities, including removal and disposal of defective equipment. The Contractor shall place fire-stop materials in conduits and pathways during an installation. Fire-Stop materials must be previously approved by local electrical and building codes. The Contractor shall notify VA when any service request, repair, or maintenance is completed. Notification shall be by telephone call or email to the VA local technical

contact. The service request, repair, or maintenance is not considered complete until a VA Facility Chief Information Officer (CIO) or designee confirms that the completion of service is acceptable.

5.6 Account records and reporting

The Contractor shall provide VA access to customer support and service records. The Contractor shall maintain accurate customer service records. Customer Service Records shall be aggregated by service delivery point with an itemized list of service types provided. Customer Service Records (CSR), the price associated with each service, shall be organized by VA parent facility. All data must have the ability for Electronic Data Interchange (EDI) in a variety of formats, i.e., MS Word, MS Excel, extensible markup language (XML), or other standard formats such as flat-files or text files. The report shall be delivered to the COR or designee by email on or about the same time every month.

6 GENERAL REQUIREMENTS

6.1 Position/task risk designation level(s) and contractor personnel security requirements

The Contractor(s) shall comply with all personnel security requirements included in this contract and local level organization security requirements described in each individual task order. All Contractor personnel who require access to VA computer systems shall be subject to background investigations and must receive a favorable background investigation from VA.

The position/task sensitivity risk designation is Low, and level of background investigation is none. 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”.

OIT requires all contractor staff to be escorted at all times by an OIT representative and as such the Contractor staff do not require background investigation as they will not be badged by the VA.

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.

6.2 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:

DRAFT

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

6.3 Performance metrics

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

Performance Objective	Performance Standard	Acceptable Performance Levels
Transition	No Loss of service.	100% of the time
Account Management	Complete visibility and access to all accounts provided to VA-only, password protected, web-based management portal	100% of the time
Telecommunication Services Restoration	Service restorations are done within 24 hours.	100% of the time
Voice and Data Services and Customer Support	Customer service representative available 24 hours/day, 7 days a week, 365 days a year.	100% of the time
Major Failure Response Time	Contractor responds to major system failures within one hour of notification.	100% of the time
Minor Failure Response Time	Contractor responds to minor system failures within four hours of notification, Monday through Friday, from 8 a.m. to 5 p.m. ET.	99.9% of the time
Service Request Response Time	Qualified technician calls requestor within one hour of a service request.	99.9% of the time
Telecommunication Availability (Uptime)	Telecommunication services are available 24 hours per day, 7 days per week.	99.9% of the time

DRAFT

VA Directive 710 (6.1.1)	The Contractor(s) shall comply with all personnel security requirements included in this contract and local level organization security requirements described in each individual task order. Contractor Technicians will require escorts in VA facilities in accordance with Section 2.h (6) of VA Directive 0710	100% of the time

6.4 Facility/resource provisions

The Contractor shall contact the COR for Government documentation needed and which is not available by other means.

The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. For detailed Security and Privacy Requirements refer to ADDENDUM A and ADDENDUM B.

6.5 Government furnished information

Government site plans, manuals, and drawings are not applicable to this acquisition.

DRAFT

7 ACRONYMS

The following is a list of acronyms that may be found in this document:

BRI – Basic Rate Interface
CLEC – Competitive Local Exchange Carrier
CIO – Chief Information Officer
DVA – Department of Veterans Affairs
FBO – Federal Business Opportunities
FFP – Firm Fixed Price
FY – Fiscal Year
GFE – Government Furnished Equipment
ILEC – Incumbent Local Exchange Carrier
ISDN – Integrated Services Digital Network
IT – Information Technology
LEC – Local Exchange Carrier
LOA – Letter of Authorization
LPTA – Lowest Price Technically Acceptable
MRC – Monthly Recurring Charges
OEC – Office of Enterprise Communications
OIT – Office of Information Technology
POP – Period of Performance
PIC – Primary Interexchange Carrier
PRI – Primary Rate ISDN
PUC Public Utilities Commission
PWS – Performance Work Statement
QOS – Quality of Service
RFI – Request for Information
RFQ – Request for Quote
ROI – Return on Investment
SDP – Service Delivery Point
SLA – Service Level Agreement
TO – Task Order
TBO – Telecommunications Business Office
TEM – Telecommunications Expense Management
TSP – Telecommunications Service Priority
TTU – Test and Turn Up
VA – Veterans Affairs
VoIP – Voice over Internet Protocol

DRAFT

ADDENDUM A

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

Each documented initiative under this contract incorporates the 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

DRAFT

Profile (TRMSP). The 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 January 18, 2017, the Architectural and Transportation Barriers Compliance Board (Access Board) revised and updated, in a single rulemaking, standards for electronic and information technology developed, procured, maintained, or used by Federal agencies covered by Section 508 of the Rehabilitation Act of 1973, as well as our guidelines for telecommunications equipment and customer premises equipment covered by Section 255 of the Communications Act of 1934. The revisions and updates to the Section 508-based standards and Section 255-based guidelines are intended to ensure that information and communication technology (ICT) covered by the respective statutes is accessible to and usable by individuals with disabilities.

A3.1 Section 508 – Information and Communication Technology (ICT) Standards:

The Section 508 standards established by the Access Board are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure ICT. These standards are found in their entirety at: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines . A printed copy of the standards will be supplied upon request.

Federal agencies must comply with the updated Section 508 Standards beginning on January 18, 2018. The Final Rule as published in the Federal Register is available from the Access Board: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule .

DRAFT

The Contractor shall comply with “508 Chapter 2: Scoping Requirements” for all electronic ICT and content delivered under this contract. Specifically, as appropriate for the technology and its functionality, the Contractor shall comply with the technical standards marked here:

☒E205 Electronic Content – (Accessibility Standard -WCAG 2.0 Level A and AA Guidelines)
☒E204 Functional Performance Criteria
☒E206 Hardware Requirements
☒E207 Software Requirements
☒E208 Support Documentation and Services Requirements

A3.2 Compatibility with Assistive Technology

The standards do not require installation of specific accessibility-related software or attachment of an assistive technology device. Section 508 requires that ICT be compatible with such software and devices so that ICT can be accessible to and usable by individuals using assistive technology, including but not limited to screen readers, screen magnifiers, and speech recognition software.

A3.3 Acceptance and Acceptance Testing

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the Section 508 Chapter 2: Scoping Requirements standards identified above.

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

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. The 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. The VA will not invalidate or make reimbursement for parking violations of the Contractor.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.

DRAFT

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 shall have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA Contracting Officer will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA Contracting Officer for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA Contracting Officer.

DRAFT

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.

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.

    e. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
    f. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
    g. 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.

DRAFT

ADDENDUM B

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

- **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.

- **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 TO.

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, the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be

DRAFT

acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

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

- **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 onsite inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

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

DRAFT

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

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

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

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

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

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

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

DRAFT

requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

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

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

- **INFORMATION SYSTEM DESIGN AND DEVELOPMENT**

1. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, *VA Information Security Program*). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6508, *VA Privacy Impact Assessment*.

2. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.

3. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also

DRAFT

use the Windows Installer Service for installation to the default “program files” directory and silently install and uninstall.

4. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

5. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

6. The Contractor/Subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.

7. The Contractor/Subcontractor agrees to:

a. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

i. The Systems of Records (SOR); and

ii. The design, development, or operation work that the Contractor/Subcontractor is to perform;

b. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and

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

8. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design,

DRAFT

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

DRAFT

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 severity of the incident.

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

- **INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE**

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

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

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

DRAFT

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

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

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

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

DRAFT

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.

DRAFT

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.

- **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.

DRAFT

- **LIQUIDATED DAMAGES FOR DATA BREACH**

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

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

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

1) Nature of the event (loss, theft, unauthorized access);
2) Description of the event, including:

a) date of occurrence;

b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;

3) Number of individuals affected or potentially affected;

4) Names of individuals or groups affected or potentially affected;

5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;

6) Amount of time the data has been out of VA control;

7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);

8) Known misuses of data containing sensitive personal information, if any;

DRAFT

9) Assessment of the potential harm to the affected individuals;

10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and

11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

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.

- **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.

- **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:

DRAFT

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

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

3) Successfully complete *Privacy and HIPAA Training* if Contractor will have access to PHI;

4) Successfully complete the appropriate VA privacy training and annually complete required privacy training; and

5) Successfully complete any additional cyber 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 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 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.

DRAFT

SCHEDULE FOR DELIVERABLES

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

Task	Deliverable ID	Deliverable Description
5.1.1	A	**Quarterly Contract Status Report** Initial report due Thirty (30) days after receipt of order (ARO), subsequent reports due quarterly. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

DRAFT