DRAFT

PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS
Office of Information & Technology
Service Delivery & Engineering

Enterprise Infrastructure Solution (EIS) Management Software

Date: 08/23/2017
TAC-17-45408
PWS Version Number: B 1.3

Contents

1.0 BACKGROUND

The Department of Veterans Affairs (VA), Office of Information and Technology (OI&T), provides telecommunications services and support VA wide. OI&T uses the Operations Support System (OSS), which is a repository for telecommunication circuit and services orders, inventory, and billing functions and inventory data for the services provided through General Service Administration's (GSA's) Networx Contract.

VA requires a software management solution that will support the GSA Enterprise Infrastructure Solutions Contract (EIS) to provide full life-cycle telecommunications asset management to include ordering, billing, inventory monitoring, and purchase order tracking and e-bonding. OI&T also seeks improvement in support, reporting, auditing, analytics and invoicing to provide the level of care required for our Veterans as well as reducing operating expenses.

2.0 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," August 2013.
4. 10 U.S.C. § 2224, "Defense Information Assurance Program".
5. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974".
6. Department of Veterans Affairs (VA) Directive 0710, "Personnel Suitability and Security Program," May 18, 2007.
7. VA Directive 6102, "Internet/Intranet Services," July 15, 2008.
8. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003.
9. OMB Circular A-130, "Management of Federal Information Resources," November 28, 2000.
10. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)".
11. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008.
12. 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.
13. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004.
14. VA Directive 6500, "Information Security Program," August 4, 2006.
15. VA Handbook 6500, "Information Security Program," September 18, 2007.
16. VA Handbook 6500.1, "Electronic Media Sanitization," March 22, 2010.

17. VA Handbook 6500.2, “Management of Security and Privacy Incidents,” June 17, 2008.
18. VA Handbook 6500.3, “Certification and Accreditation of VA Information Systems,” November 24, 2008.
19. VA Handbook, 6500.5, Incorporating Security and Privacy in System Development Lifecycle.
20. VA Handbook 6500.6, “Contract Security,” March 12, 2010.
21. Technical Reference Model (TRM) (reference at http://www.va.gov/trm/)
22. National Institute Standards and Technology (NIST) Special Publications
23. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008.
24. VA Directive 6300, Records and Information Management, February 26, 2009.
25. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010.

3.0 SCOPE OF WORK

This is an acquisition for management software that will interoperate with the General Services Administration (GSA) Enterprise Infrastructure Solutions Contract (EIS). The vendor shall provide Commercial off the shelf (COTS) software to achieve full EIS lifecycle asset management to include ordering, billing, inventory monitoring, and purchase order tracking and e-bonding. The COTS software shall be configured, tested and accepted for use by the VA within 30 calendar days after award. The EIS management software shall be capable of integration with the EIS Vendor Portals within 45 calendar days after award. Training for up to 100 users and up to 10 software administrators shall be completed by the Contractor. The Contractor shall provide all labor, management, tools, and material to perform all requirements cited in this PWS.

4.0 PERFORMANCE DETAILS

4.1 CONTRACT TYPE

This is a Firm Fixed Price (FFP) Award order

4.2 PERFORMANCE PERIOD

The period of performance shall be for a base period of 12 months from date of the award, with four (4) 12-month option periods.

Installation, maintenance, and disconnection of services shall take place between 8:00 AM to 4:30 PM (Local Time), Monday through Friday, excluding Federal holidays. Work may be required outside of normal business hours due to business requirements.

There are 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

4.3 PLACE OF PERFORMANCE

The Contractor shall remotely deploy the VA EIS management software on equipment at VA locations . The software configurations for the equipment at these VA locations is provided upon award. The Contractor shall not provide any onsite maintenance.

4.4 TRAVEL

The Government does not anticipate travel to perform the tasks associated with this effort. If the Contractor requires travel to perform any of these tasks, the Contractor shall include all estimated travel costs in its firm-fixed price line items. These costs shall not be directly reimbursed by the Government.

5.0 SPECIFIC TASKS AND DELIVERABLES

5.1 REPORTING REQUIREMENTS

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall deliver an overall Contractor Project Management Plan (CPMP) that lays out the Contractor’s approach, timeline and tools to be used in execution of this order. The CPM should take the form of both a narrative and graphic format that displays the schedule, milestones, risks and resource support. The CPM shall also include how the Contractor shall coordinate and execute data collection requests as identified within the PWS. The initial baseline CPMP shall be concurred upon by VA and updated monthly thereafter. The Contractor shall update and maintain the VA PM approved CPMP throughout each period of performance.

Deliverables:

A. Contractor Project Management Plan

5.1.2 QUARTERLY STATUS REPORT

The Contractor shall prepare and submit a Quarterly Status Report in Microsoft (MS) Word or Excel format.

For each Status Report, indicate/discuss:

1. Performance metrics
2. Critical items for Government review
3. Accomplishments
4. Significant open issues, risks and mitigation actions
5. Summary of issues closed
6. Projected activities for next reporting period

Deliverable:

A. Quarterly Status Report

5.1.3 IMPLEMENTATION REPORT

This Contractor shall prepare and submit a weekly Status Report in MS Excel format. This report shall convey the status of EIS management software. The content requirements are the same as in section 5.1.1.

Deliverable:

A. Weekly Implementation Status Report

5.2 MEETING REQUIREMENTS

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

5.2.1 TASK ORDER KICKOFF MEETINGS

The Contractor shall hold a kickoff meeting within five business days after TO award unless otherwise specified by the Government. At a minimum, the Contractor shall present, for review and approval by the Government, the details of the intended approach, work plan, and project schedule for each effort. This shall be a virtual meeting. Dates, locations, and agenda shall be specified at least two calendar days prior to the meeting. The Contracting Officer (CO), Contract Specialist (CS), The Contracting Officers Technical Representative (COTR), and VA Project Manager (PM) shall be invited at a minimum. The Contractor shall provide a kick off presentation at

the meeting and any pertinent information regarding the meeting within one day after the meeting is held.

Deliverable:

A. Task Order Kickoff Presentation

5.2.2 PROGRAM PROGRESS REVIEWS (BASE CONTRACT LEVEL)

The Contractor shall conduct Program Progress Reviews (PPR) for Government personnel. This will be a virtual meeting. The CO/CS or the COR will schedule the initial PPR. It is anticipated the first PPR will occur no later than 90 calendar days after date of award. Thereafter, PPRs shall occur quarterly, for the life of the order. 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.
5. New technologies that would benefit VA.

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.

Deliverable:

A. Program Progress Reviews

5.3 EIS MANAGEMENT SOFTWARE

5.3.1 UPTIME

The Software shall be capable of continuous operation (i.e. 24x7) not related exclusions defined in section 5.4.2.3.

5.3.2 MANAGEMENT SOFTWARE REQUIREMENTS (SYSTEM)

1. The EIS management software shall have the capability to provide unique reports in each of its modules; Service Request, Preorder, Order, Inventory, Billing and Administrative. The unique reports required are: Ordering Reports, Billing Reports, Inventory Reports, Notification Reports, and System Logging Reports (User Access).
2. The EIS management software shall load monthly EIS invoices for the purposes of generating an error report using unique algorithms designated by OI&T. The system shall use the algorithms to generate an error report monthly.
3. The system shall be configured for up to 10 administrators and 100 users.

4. The system shall allow designated users (billing analysts) to submit disputes through the system to the EIS Vendor.
5. The system shall allow designated users to make corrections to inventory and ordering items in the system to reconcile the Vendor's billing and inventory with what the Agency ordered.
6. The system shall allow discretionary controls for users such as contractors who will create orders and disputes on behalf of the Government. The controls shall also restrict the same users from submitting orders.
7. The system shall provide an activity queue (work queue) for Designated Agency Representatives (DAR) to review contractor or field user activities such as price quotes, orders, and disputes. The system shall allow the DAR to approve activities within their queue and submit orders and disputes created by other users to EIS vendors.
8. The system shall allow a user to input price quotes and service orders for all services provided by each Vendor under the EIS Contract.
9. The system shall be able to change pricing for each vendor per the EIS contract. In addition, the system shall allow for the input of Individual Case Based (ICB) pricing at the price quite level and shall generate annual ICB price changes at the CLIN level.
10. The system shall provide a consolidated inventory based on the Unique Billing Identifier (UBI) or EIS UBI or a consolidated inventory for each of the EIS vendors. The system shall have functionality that allows a designated user to make corrections to reconcile services that were ordered against services the vendor is billing for.
11. The system shall have a user administration module that gives designated OI&T users the capability to assign unique roles for sub-users. The unique role assignments must include discretionary access functionality at the Account Billing (AB) Code and each of the 28 characters (seven quadrants) of VA hierarchy code. Discretionary access capability shall also include subsets of system modules such as: the ability for a user to only access price quote generation, the ability for a user to only access price quote approval, the ability for a user to only access billing information, inventory information, ordering information, or notification information. This system will also have the capability for discretionary hierarchy code access at the module level.
12. The system shall have the functionality to provide discretionary access controls for multiple contracts.
13. The system shall allow a designated OI&T user (administrator) to add and remove unique menus and selections to the menus in each of the system's modules. The Agency system administrator shall be allowed to add sub features of specific telecommunications services to Additional Data Object (ADO) fields.
14. The system shall allow for Electronic Ordering that provides the ability to convert all voice/data and other telecommunications service requests into service orders that the DAR can submit to their suppliers through a variety of electronic ordering mechanisms and e-bonding (for those carriers supporting electronic ordering) as

well as support electronic processing of Firm Order Commitment (FOC) and Service Order Completion (SOC) notices generated by EIS carriers (for those EIS awardees supporting electronic processing of these notices).

15. The system shall accept Vendors' electronic invoices in accordance with the GSA EIS contract to be loaded into the EIS management software.
16. The system shall to input up to 400 Automatic Number Identification (ANI)s at a time without doing multiple service order requests.
17. Notifications shall be uploaded into the system via Extensible Markup Language (XML).
18. The system shall have a Queue Manager for assigning new services orders request.
19. The system shall submit and create Agency Hierarchy Code (AHC)'s via electronic interface. There are up to 7500 hierarchy. The system shall accommodate and manage those AHCs including creation, disablement, and modification, and communicate those changes electronically to the EIS vendors.
20. The system shall support the GSA EIS contract by comparing inventory to billing invoices.
21. The system shall be delivered, tested and accepted within 30 days after award.
22. The system software shall reside on Government equipment and be remotely installed and maintained.

5.3.3 SOFTWARE ANALYTICS

The EIS management software shall have an ad-hoc reporting tools that can be modified by the OI&T users to show spending and trending as well as inventory count, trends, and status. The Vendor software shall have an administrative level dashboard that can configured to show business analytics via chart or graph and allow configured data to be displayed in electronic media. Acceptable electronic media include: Microsoft (MS) Word, MS Excel, MS PowerPoint, and Adobe Postscript Data Format (PDF).

5.3.4 TRAINING

The Contractor shall provide training for up to 100 users and up to 10 software administrators shall be completed by the Vendor within 5 business days before the integration of the new EIS COTS management software. Training location shall be virtual.

5.4 SERVICE LEVEL AGREEMENT (SLA)

The Contractor software and services shall conform to SLA parameters as defined in the following sub-paragraphs. These SLA's shall apply from the Government Acceptance Date for the duration of the agreement term.

5.4.1 CONTRACTOR CUSTOMER SUPPORT

The Contractor shall use an Escalation Process to resolve customer service issues and provide a single POC for each issue or dispute. The Contractor shall provide the COR an Escalation Process 14 calendar days after software installation outlining the specific steps taken to resolve customer service issues. The escalation list shall be updated within 5 calendar days after any change of contractor key personnel.

The Contractor shall provide the COR a Customer Support Organization Chart containing employee names, email addresses, and direct phone numbers.

The Contractor shall provide technical Help Desk support. Technical Help Desk support is required 7AM to 7PM during regular business hours. A Vendor staffed telephone number shall be designated as the primary help number for VA EIS Administrators to call to report a problem and have a Trouble Ticket assigned. Automated answering or ticket automation service shall not be an acceptable solution. The Contractor's customer service representative shall be in the Continental United States (CONUS) and 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 software fault or a failure to meet a SLA. A unique Trouble Ticket reference number shall be given to the Government representative and 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 software.

The Contractor shall provide the COR a monthly report of Help Desk trouble tickets at the completion of each billing cycle. The Help Desk report shall contain all tickets opened during the billing cycle and shall include a list of trouble ticket numbers and the software fault, time of trouble ticket report, time of software restoration, and description of fault and resolution of fault.

Deliverables:

A. Escalation Process Plan
B. Customer Support Organization Chart
C. Monthly Help Desk Report

5.4.2 MEAN TIME TO REPAIR (MTTR)

MTTR is the average time for the Contractor to restore the software failure. The SLA for MTTR shall be four hours for failure and five business days for partial software degradation. The Contractor shall provide technical support/resolution to assist VA with issues pertaining to EIS management software. MTTR times begin when the Contractor receives a support request from VA. The Contractor shall respond to VA's support requests per the following fault classifications.

5.4.2.1 PRIORITY 1– FAILURE OF SOFTWARE

A failure is defined as an unscheduled period in which the software is unavailable for use by the VA for 10 or more minutes, not related exclusions defined in section 5.4.2.3. The Contractor shall respond to all failure of software requests within four hours. Notifications shall be provided to the VA POC every two business hours via telephone until restored. The MTTR for Priority 1 help desk reports is four hours.

5.4.2.2 PRIORITY 2– PARTIAL SOFTWARE DEGRADATION

Partial software degradation means VA's workflow is not seriously affected or limited including reporting tools that cannot generate outputs. The Software Vendor shall respond to all Partial software degradation reports within four hours. Status notifications shall be provided to VA POC every business day via telephone until restored. The MTTR for Priority 2 help desk reports is five business days.

5.4.2.3 EXCLUSIONS

The MTTR SLA does not apply due to VA facilities outage or VA hardware and software outage or maintenance. The SLA does not apply until after acceptance of the management software by the Government. The SLA does not apply during scheduled maintenance of the EIS management software. The Vendor shall notify VA POC three business days in advance of any scheduled maintenance that may impact the operation of the EIS management software. The Vendor shall describe in detail how long and to what level degraded software performance is to be expected. The Contractor shall obtain approval in advance from the VA POC before scheduled maintenance occurs. The software shall not 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 related to VA Facilities and hardware and software maintenance.

6.0 GENERAL REQUIREMENTS

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

6.1.1 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:

Table 1

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.1	X		
5.2	X		
5.3			X
5.4	X		

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 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.

6.1.2 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 can 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 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.

Deliverable:

A. Contractor Staff Roster

6.2 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B. Acceptable electronic media include: Microsoft (MS) Word, MS Excel, MS PowerPoint, 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. All Performance levels are for calendar month and are not cumulative.

Table 2

Performance Objective	Performance Standard	Acceptable Performance Levels
Software uptime (5.3.1)	The Software shall function 24 hours per day, 7 days per week, and 365 days per year.	99.9% uptime
Service Level Agreement (5.4)	Mean Time to Repair	MTTR shall be four hours for failure and five business days for software degradation
Position/Task Risk Designation Level(s) and Contractor Personnel Security Requriements (6.1)	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

A Performance Based Service Assessment Survey will be used in combination with the Quality Assurance Surveillance Plan (QASP) to assist the Government in determining acceptable performance levels.

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 System Security Plans (SSP) and Authority to Operate (ATO) 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

All Government furnished information shall be returned at the competition of the contract.

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

published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

Section 508 – Electronic and Information Technology (EIT) Standards:
The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: http://www.section508.gov and http://www.access-board.gov/sec508/standards.htm. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

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

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the EIT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

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.

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.

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.

ADDENDUM B

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

B1. GENERAL

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

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

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

resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

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

B3. VA INFORMATION CUSTODIAL LANGUAGE

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

2. VA information should not be co-mingled, if possible, with any other data on the 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 days of termination of the contract.

4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to VA information or information systems

after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

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

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

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

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

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

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

11. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection

with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

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

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

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

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

3. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default “program files” directory and silently install and uninstall.

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

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

Information Security Program and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

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

7. The Contractor/Subcontractor agrees to:

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

i. The Systems of Records (SOR); and

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

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

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

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

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

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

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

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

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

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

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

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS,

and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must be reviewed and approved by VA prior to implementation.

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

c. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization) (C&A) of the Contractor's systems in accordance with VA Handbook 6500.3, *Certification and Accreditation* and/or the VA OCS Certification Program Office. Government-owned (Government facility or Government equipment) Contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

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

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

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

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

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

1) Vendor must accept the system without the drive;

2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or

3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;

a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and

b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.

c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

B6. SECURITY INCIDENT INVESTIGATION

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

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

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

d. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law

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

B7. LIQUIDATED DAMAGES FOR DATA BREACH

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

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

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

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

a) date of occurrence;

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

3) Number of individuals affected or potentially affected;

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

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

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

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

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

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

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

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

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

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

B8. SECURITY CONTROLS COMPLIANCE TESTING

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

General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

B9. TRAINING

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

1) 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.