PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS
National Cemetery Administration
Office of Management
Business Transformation and Requirements Service

National Cemetery Administration Kiosks
Purchase/Installs and Maintenance Support

Date: June 13, 2017

Contents

1.0 BACKGROUND

The Department of Veterans Affairs (VA), Office of Information and Technology (OIT) CDCO, Quantico Information Technology Center (QITC) is responsible for providing information technology support to VA's National Cemetery Administration (NCA) throughout the continental United States (CONUS), outside the continental United States (OCONUS), and Puerto Rico.

NCA's mission is to honor the military service of our nation's Veterans. NCA provides a dignified burial and lasting memorial for Veterans and their eligible family members. National Cemeteries are maintained as national shrines. NCA's vision is to provide a lasting tribute to our nation's Veterans by being mission driven, results oriented, and customer focused. NCA accomplishes this goal, in part, by scheduling burials and maintaining National Cemeteries. It processes applications for Veteran headstones and markers for placement in National Cemeteries, State Veterans Cemeteries, National Park Service Cemeteries, United States Army Post Cemeteries, and other cemeteries. NCA also administers the State Veterans Cemetery Grants Program, which complements the network of National Cemeteries, and provides Presidential Memorial Certificates (PMCs) to next of kin of deceased Veterans.

In 1997, the NCA used in-house resources to develop and maintain a grave locator/general information kiosk application as part of its commitment to implement cost-effective customer service improvements and facilitate cemetery administrative processes. The application is designed to run 24 hours a day, seven days per week. It allows visitors to find the exact location of individuals interred at the cemetery; provides the visitor with a cemetery map for use in locating gravesites; and displays the most frequently sought information, including: the cemetery's operating hours, upcoming events, grounds/floral policy, cemetery history, military funeral honors policy, burial eligibility information, and NCA rules and regulations.

NCA presently has 104 kiosks in use. Currently, all 104 existing kiosks are covered under a maintenance agreement.

2.0 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this 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. 10 U.S.C. § 2224, "Defense Information Assurance Program"
4. Software Engineering Institute, Software Acquisition Capability Maturity Modeling (SA CMM) Level 2 procedures and processes
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,” June 4, 2010
8. VA Directive 6102, “Internet/Intranet Services,” July 15, 2008
9. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards”
10. OMB Circular A-130, “Managing Federal Information as a Strategic Resource,” July 28, 2016.
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): Policies for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.
15. VA Directive 6500, “Managing Information Security Risks: VA Information Security Program,” September 20, 2012.
16. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: Information Security Program,” March 10, 2015.
17. VA Handbook 6500.1, “Electronic Media Sanitization,” November 3, 2008.
18. VA Handbook 6500.2, “Management of Breaches Involving Sensitive Personal Information,” July 28, 2016.
19. VA Handbook 6500.3, “Assessment, Authorization and Continuous Monitoring of VA Information Systems,” February 3, 2014.
20. VA Handbook, 6500.5, “Incorporating Security and Privacy into the System Development Life Cycle,” March 22, 2010.
21. VA Handbook 6500.6, “Contract Security,” March 12, 2010.
22. Project Management Accountability System (PMAS) portal (reference PWS References -Technical Library at https://www.voa.va.gov/)
23. OIT ProPath Process Methodology (reference PWS References -Technical Library and ProPath Library links at https://www.voa.va.gov/) NOTE: In the event of a conflict, OIT ProPath takes precedence over other processes or methodologies.
24. National Institute Standards and Technology (NIST) Special Publications
25. VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment, October 15, 2014.
26. VA Directive 6300, Records and Information Management, February 26, 2009.
27. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010.

3.0 SCOPE OF WORK

The Contractor shall provide kiosk enclosures as well as delivery, installation, warranty, maintenance, and support to OCONUS, CONUS, and Puerto Rico VA National Cemetery sites.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The contract-ordering period shall be five-years beginning from date of award. All orders shall be placed within the ordering period. Specific periods of performances shall be identified in each order, and may exceed the order period up to 12 months. The Contractor is not required to deliver or install kiosks on Federal holidays. However, maintenance shall be provided 365 days per year.

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

Under current definitions, four are set by date:

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

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

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

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

4.2 PLACE OF PERFORMANCE

Tasks under this PWS shall be performed at VA National Cemeteries located throughout the OCONUS, CONUS, and Puerto Rico. A list of cemetery locations is provided in Attachment 2.

4.3 TRAVEL

The Government anticipates travel under this effort to perform the tasks associated with the effort, as well as to attend program-related meetings or conferences through the ordering period. All travel related costs shall be included in the firm-fixed price line items. These costs will not be directly reimbursed by the Government.

5.0 SPECIFIC TASKS AND DELIVERABLES

5.1 PROJECT MANAGEMENT

5.1.1 PROJECT MANAGEMENT PLAN

Within three business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations. The roster shall contain the Contractor's Full Name, Full Social Security Number, Date of Birth, Place of Birth, and individual background investigation level requirement (identified in Section 6.2). Additional requirements regarding the background investigation process are identified in section 6.3. The Contractor shall deliver a Project Management Plan (PMP) 10 days after contract award that lays out the Contractor's approach, timeline, and tools to be used in execution of the contract. The PMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks, and resources. The PMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The Contractor shall attend a kick-off meeting telecom within two weeks of contract award to discuss the PMP and the status of background investigations. The initial baseline PMP shall be concurred upon and updated monthly thereafter. The Contractor shall update and maintain the VA PM approved PMP throughout the period of performance.

Deliverable:
A. Project Management Plan
B. Staff Roster

5.1.2 MONTHLY REPORTING REQUIREMENTS

The Contractor shall provide a Monthly Progress Report of all task order activities including repairs and equipment replacement. The Monthly Progress Report shall include detailed explanations of repair work initiated or completed each month and shall accurately reflect all required data elements. The Contractor shall include in the report descriptions of all repairs made to kiosks and IT components and describe all replacements made including type of component repaired/replaced, location, status, service dates, and serial number for all repaired, replaced, and newly installed equipment. The Contractor shall also include components coming to end of life (five years after original purchase date) in the following three-month period. These reports shall reflect data as of the last day of the preceding month. It is expected that the Contractor will keep in communication with VA so that issues that arise are transparent to both parties.

Deliverable:
A. Monthly Progress Report

5.2 KIOSK CONFIGURATION

The Contractor shall provide a through the wall kiosk enclosure and a freestanding indoor kiosk enclosure. The Contractor shall provide kiosks that deter/discourage damage by theft, vandalism, or misuse of the enclosure and its IT equipment. The kiosks must meet established standards and VA requirements including Section 508 compliance. The Government will provide a Dell Laptop Computer E6320 or Equivalent at time of delivery to be included in all kiosk enclosures.

5.2.1 THROUGH THE WALL KIOSK ENCLOSURE

The Contractor shall provide a through the wall kiosk enclosure with the following minimum specification and miscellaneous component part requirements:

A. Kiosk Dimensions: 27.0 inches wide, 45.0 inches high, and 26.0 inches deep
B. The kiosk must include a touch screen that can operate in temperatures from 0 degrees Celsius to 40 degrees Celsius (32 degrees Fahrenheit to 104 degrees Fahrenheit), and a humidity of 20 percent to 80 percent non-condensing
C. The kiosk must also include a thermal printer that can operate in temperatures from 5 degrees Celsius to 40 degrees Celsius (41 degrees Fahrenheit to 104 degrees Fahrenheit), and a humidity of 20 percent to 85 percent non-condensing
D. Power surge device
E. Dell Laptop Computer E6320 or Equivalent (to be provided by Government)
F. Two rolls thermal printer paper, 8.47” W x 640’ L inside-wound thermal paper w/1.51” inside core
G. 25” network cable (4 pair 100-ohm high performance, stranded conductor, unshielded twisted pair cable, meeting or exceeding the Category 6 specifications, RJ-45 male connectors on both ends)
H. One package of cleaning wipes that are touch screen manufacturer approved
I. Lock with two keys
J. Constructed of stainless steel with cast aluminum signage

Deliverable:

A. Kiosk and Keys

5.2.2 FREESTANDING INDOOR KIOSK ENCLOSURE

The Contractor shall provide a freestanding indoor kiosk enclosure with the following minimum specification and miscellaneous component part requirements:

A. Dimensions: 25.0 inches wide, 48.0 inches high, and 26.0 inches deep
B. The kiosk must include a touch screen that can operate in temperatures from 0 degrees Celsius to 40 degrees Celsius (32 degrees Fahrenheit to 104 degrees Fahrenheit), and a humidity of 20 percent to 80 percent non-condensing
C. The kiosk must also include a thermal printer that can operate in temperatures from 5 degrees Celsius to 40 degrees Celsius (41 degrees Fahrenheit to 104 degrees Fahrenheit), and a humidity of 20 percent to 85 percent non-condensing
D. Power surge device

E. Dell Laptop Computer E6320 or Equivalent (to be provided by Government)
F. Two rolls thermal printer paper, 8.47" W x 640' L inside-wound thermal paper w/1.51" inside core
G. 25" network cable (4 pair 100-ohm high performance, stranded conductor, unshielded twisted pair cable, meeting or exceeding the Category 6 specifications, RJ-45 male connectors on both ends)
H. One package of cleaning wipes that are touch screen manufacturer approved at installation
I. Lock with two keys
J. Constructed of wood with laminate finish and vinyl signage

Deliverable:
A. Kiosk and Keys

5.3 KIOSK ENCLOSURE INSTALLATION

The Contractor shall install and set up an estimated 50 Kiosks (10 per year) throughout the entire ordering period of the contract. The Contractor shall install Kiosks no later than 60 days after receipt of task order. The Government will ensure the building has the appropriate configuration and electrical/networking cabling required for all kiosk configurations described in 5.2. The Contractor shall submit a site plan detailing all requirements associated with the installation of a kiosk within 7 days after receipt of task order. The site plan shall include any Government required construction related activities necessary in order for the Contractor to complete the installation. Construction related activities are defined as any alteration of real property. The COR will review and approve/disapprove site plans prior to any work being done. The Contractor shall provide network cables at each location. Upon delivery of a kiosk, the Government will provide the laptop required for the kiosk configuration. The Contractor shall test and demonstrate each kiosk is operational after setup and installation. The Contractor shall supply the cemetery with two keys to the kiosk enclosure doors after installation / enclosure setup. The Contractor shall inspect installed enclosures and apply touch up paint to the kiosk enclosure as needed. The leftover paint shall remain with the cemetery. All kiosks enclosures and kiosk components shall include a warranty for one year beginning the date of acceptance. Warranty requirements are the same as defined below in Section 5.4 Kiosk Maintenance and Help Desk Support.

5.3.1 THROUGH THE WALL KIOSKS

The Contractor shall furnish all labor, materials, supplies, and tools necessary to deliver and install through-the-wall kiosk enclosures. The Government will ensure the building has the appropriate size opening and electrical/networking cabling required for a through the wall kiosk configuration described in 5.2.1.

5.3.2 FREESTANDING KIOSKS

The Contractor shall furnish all labor, materials, supplies, and tools necessary to provide and install freestanding kiosk enclosures. A freestanding kiosk enclosure shall be installed to sit level on varying types of flooring such as linoleum, carpet, wood, brick, and concrete.

5.3.3 INSTALLATION REPORTS

The Contractor shall provide an Installation Report with part numbers, serial numbers, and manufacturer numbers for all kiosk equipment including IT equipment and software after completing a kiosk installation. The Contractor shall complete all warranty information (registration cards) in conjunction with the installation of a kiosk enclosure.

Deliverable:
A. Installation Report

5.3.4 KIOSK USER GUIDE

The Contractor shall provide hard copy Kiosk User Guides to cemetery personnel. The Kiosk User Guide shall contain cemetery specific and enclosure specific instructions on the operations of the kiosk and installation. The instructions shall include:

A. Turning the kiosk on and off, including all component equipment,
B. Trouble-shooting tips to facilitate continuous operation of the kiosk and components,
C. Help-desk contact information.

Deliverable:
A. Kiosk User Guide

5.4 KIOSK MAINTENANCE AND HELP DESK SUPPORT

The Contractor shall maintain, repair, and replace kiosks and kiosk components for 104 existing and future new kiosks to ensure kiosks are operational. The Contractor shall diagnose and correct malfunctions associated with the kiosks and kiosk components. The Contractor shall provide repairs during cemetery business hours, 5 days a week (Monday to Friday) as necessary to ensure failed kiosks are operational within 48 hours of a reported failure not inclusive of weekends. The Contractor shall contact the Government – QITC and NCA Business Requirements Office COR to report any issues that cause a kiosk to be non-operational for more than 48 hours. The Contractor shall repair or replace kiosk enclosures when it can no longer protect internal equipment from unauthorized access or external environmental elements. The Contractor shall also provide touch up paint and additional cleaning wipes that are touch screen manufacturer approved when requested by the COR.

The Contractor shall provide a standalone configuration solution and maintenance for kiosks that have no internet connection. The solution includes customized software, installation and support for the kiosk and the following:

- Laptop from VA (Windows 7 Home Premium or higher, with administrative login information)

- USB flash drive from VA (with login information)

- Cemetery BOSS # (3 digit Station ID)

- Cemetery data file added to the nightly extract to the VA FTP server

- Map image (jpeg file) from VA

- Contact name and email for the person who should receive the burial data updates via email

The Contractor shall provide a Help Desk for Kiosk Support 24 hours per day, seven days a week, 365 days a year. The Contractor shall respond (IAW performance standards as indicated in Section 6.5 below) to email and telephone inquiries to manage service tickets submitted by cemetery personnel.

Maintenance includes: replacement of faulty touch screens, printers, surge protectors and fans; on-site technician for touch screen replacements; custom-manufactured touch screen retrofit kits for pre-2007 kiosks; replacement of ITK38 printers as required for laptop upgrades.

Free-standing kiosks enclosures obtained prior to 2007 are not covered. However, the components are covered (listed as the alphabetized items under 5.2 Kiosk Configurations). Damages caused by accidents, vandalism, or natural disasters are covered.

Deliverable:
A. Maintenance Report**:** The Contractor shall provide a report of maintenance activities in the Monthly Report for all maintenance related activities with part numbers, serial numbers, and manufacturer numbers. The Contractor shall update any warranty information (registration cards) in conjunction with the maintenance of a kiosk enclosure.

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

The Contractor shall support VA efforts in accordance with the specified project management system that mandates all new VA IT projects/programs use an incremental development approach, requiring frequent delivery milestones that deliver new capabilities for business sponsors to test and accept functionality. Implemented by the Assistant Secretary for IT, Veteran-Focused Integration Process (VIP) is a VA-wide initiative to better empower the OIT Project Managers and teams to meet their mission: delivering world-class IT products that meet business needs on time and within budget.

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

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

The Tasks identified below and the resulting Position Sensitivity and Background Investigation delineate the Background Investigation requirements by Contractor individual, based upon the tasks the particular Contractor individual will be working. The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each individual, based upon the tasks the Contractor individual will be working.

Position Sensitivity and Background Investigation - The position sensitivity and the level of background investigation commensurate with the required level of access for task(s) 5.1 to 5.4 within the PWS is:

☒ Moderate/MBI

6.3 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

A. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak, and understand the English language.
B. The Contractor shall bear the expense of obtaining background investigations.
C. Within three business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations. The roster shall contain the Contractor's Full Name, Full Social Security Number, Date of Birth, Place of Birth, and individual background investigation level requirement (based upon Section 6.2).
D. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
E. For Moderate or High Risk the following forms are required to be completed: 1. VA Form 0710; and 2. DVA Memorandum – Electronic Fingerprints. These should be submitted to the COR within five business days after award.
F. The Contractor personnel will receive an email notification from the Security and Investigation Center (SIC); through the Electronics Questionnaire for Investigations Processes (e-QIP) identifying the website link that includes detailed instructions regarding completion of the investigation documents (SF85, SF85P, or SF 86). The Contractor personnel shall submit all required information related to their background investigations utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP).
G. The Contractor is to certify and release the e-QIP document, print and sign the signature pages, and send them to the COR for electronic submission to the SIC. These should be submitted to the COR within three business days of receipt of the e-QIP notification email.
H. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
I. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or "Closed, No Issues" (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).
J. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
K. Failure to comply with the Contractor personnel security investigative requirements may result in termination of the contract for default.

6.4 METHOD AND DISTRIBUTION OF DELIVERABLES

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

6.5 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
Repair/resolve kiosk failures to make kiosk operational	Kiosks operational within 48 hours (excluding weekends) of reported failure	90% of the time
Submit Accurate and Timely Monthly Reports	Submitted report contains all data elements required and submitted by the 10th calendar day after the prior monthly reporting period.	90% of the time measured on a monthly basis
Respond to NCA/QITC Help Desk issues	Response received within 4 business hours of Help Desk notification	95% of the time

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 PWS language, conditions, laws, and regulations. All VA data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the COR, 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.

Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COR, CO, the 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 identified on the current external VA training site, the Employee Education System (EES), and will be tracked therein. The EES may be accessed for SSOi users within the VA network: Log-on to the VA Talent Management System (VA TMS) from any computer with Internet access at: https://logon.iam.va.gov/affwebservices/public/saml2sso?SPID=https://www.tms.va.gov/learning&RelayState=https://www.tms.va.gov/learning/user/ssoLogin.do. Non-SSOi users outside the VA network: Log-on to the VA Talent Management System (VA TMS) from any computer with Internet access at https://www.tms.va.gov.

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 VA 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 VA 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.section508.gov/acquisition-regulations. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

- ☐ § 1194.21 Software applications and operating systems
- ☐ § 1194.22 Web-based intranet and internet information and applications
- ☐ § 1194.23 Telecommunications products

- ☒ § 1194.24 Video and multimedia products
- ☒ § 1194.25 Self-contained, closed products
- ☐ § 1194.26 Desktop and portable computers
- ☒ § 1194.31 Functional Performance Criteria
- ☒ § 1194.41 Information, Documentation, and Support

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 under any conditions.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

A5.0 Confidentiality and Non-Disclosure

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

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

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA 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.
   e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.

f. Contractor PM and VA PM are informed within twenty-four hours of any employee termination.

g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)."

h. Contractor does not require access to classified data.

8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.

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 task order.

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

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

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed 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's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures comply 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 the 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's 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's 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 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**,** but in no event longer than 2 days.

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 within 2 days*.*

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's 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 VA's POA&M management process. The Contractor/Subcontractor must use VA's 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 VA's network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, PWS, or contract. All of the security controls required for Government furnished equipment (GFE) must be 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 the VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

1) Notification;
2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
3) Data breach analysis;
4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
5) One year of identity theft insurance with $20,000.00 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-day's 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 *VHA Privacy Policy 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.