SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS
Office of Information & Technology

Commodities Enterprise Contract (CEC)

Date: November 29, 2012

PWS Version Number: 21

Contents

1.0 BACKGROUND

The Department of Veterans Affairs (VA) maintains a complex information technology (IT) enterprise architecture. The VA is seeking to establish a Commodities Enterprise Contract (CEC) arrangement that will ensure standardization of commercial IT hardware and associated installation, configuration, warranty, maintenance and technical support services solutions across the VA Enterprise. The task requirements described herein seek to not only ensure standardization, but interoperability with existing hardware infrastructure, while also leveraging the VA's purchasing power as a large enterprise. The IT Hardware Commodity purchases contemplated for this effort are as follows: end user devices (such as laptops and thin clients), mobile tablets, servers, networking appliances (switches/routers), storage arrays/storage appliances, and security platforms; all of which are as identified in Section 6.0 and detailed in the applicable technical specifications attached hereto. Although not required, the Government desires that Offerors propose (1) Original Equipment Manufacturer (OEM) for those products identified in PWS paragraphs 6.4 and 6.6, and as minimal OEMs as possible for those products identified in PWS paragraph 6.1. However, Offerors shall propose one (1) OEM for those products identified in PWS paragraphs 6.3 and 6.5. Additionally, the following services are also contemplated: installation, warranty support, and incidental technical support services such as site surveys, custom installation, training, and application support.

2.0 APPLICABLE DOCUMENTS

Documents referenced in or applicable to this Performance Work Statement (PWS) are listed below. 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. FIPS Pub 201, "Personal Identity Verification of Federal Employees and Contractors," March 2006.
4. 10 U.S.C. § 2224, "Defense Information Assurance Program."
5. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974."
6. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964."
7. Department of Veterans Affairs (VA) Directive 0710, "Personnel Suitability and Security Program," September 10, 2004.
8. VA Directive 6102, "Internet/Intranet Services," July 15, 2008.
9. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003.
10. OMB Circular A-130, "Management of Federal Information Resources," November 28, 2000.
11. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)."
12. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, March 2005.
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).
15. VA Directive 6500, "Information Security Program," August 4, 2006.

16. VA Handbook 6500, "Information Security Program," September 18, 2007.
17. VA Handbook, 6500.5, Incorporating Security and Privacy in System Development Lifecycle.
18. VA Handbook 6500.6, "Contract Security," March 12, 2010.
19. Program Management Accountability System (PMAS) portal (reference PWS References - Technical Library at https://www.voa.va.gov/).
20. 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, ProPath takes precedence over other processes or methodologies.
21. Technical Reference Model (TRM) (reference at http://www.ea.oit.va.gov/Technology.asp).
22. National Institute Standards and Technology (NIST) Special Publications.

3.0 SCOPE OF WORK

The VA requires commercial IT solutions (comprised of hardware and incidental services) to improve efficiency and productivity. The VA seeks to take advantage of technological advances and new business practices that promise to increase productivity and/or reduce costs while ensuring interoperability with the VA's existing hardware infrastructure. The task requirements described herein shall support the IT needs of VA programs, Initiatives, and other requirements throughout the VA enterprise. The IT Hardware commodities included in this acquisition consist of end user devices (such as laptops and thin clients), mobile tablets, servers, networking appliances (switches/routers), storage arrays/storage appliances, and security platforms; all of which are discussed in Section 6.0 and detailed in the applicable technical specifications attached hereto. Ancillary and/or incidental hardware, software, and services required for successful implementation may be acquired via any resulting contract vehicle and are detailed in Sections 9.0, and 10.0 of this document. The VA may purchase IT Hardware Commodity items or total IT solutions. All IT Hardware Commodity items shall be available for purchase. No leasing is contemplated by this acquisition. As VA's Enterprise Architecture continues to evolve, changes and/or updates to the products offered may be necessary to ensure compliance with Enterprise Architecture approved initiatives. These changes and updates will be incorporated into CEC through Technology Refresh and/or Technology Insertion, which are discussed in paragraphs 5.1.8 and 5.1.9, respectively.

4.0 PERFORMANCE DETAILS

This is a competitive acquisition for the award of multiple Indefinite Delivery, Indefinite Quantity (IDIQ) Contracts from which Firm Fixed Priced and/or Time and Materials Delivery Orders, or a combination thereof, shall be competed and issued, unless an exception to fair opportunity is otherwise justified.

4.1 PERFORMANCE PERIOD

The ordering period for the IT Hardware Commodity products and services described herein shall be for five (5) years from date of award. However, because performance of each Delivery Order awarded prior to Contract expiration may require continued warranty and technical support services as described in Section 9.0, warranty technical support services may be performed for a maximum of five (5) years after the expiration of the five (5) year ordering period.

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

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

Under current definitions, four (4) 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 the preceding Friday shall be observed as a holiday. Similarly, if one falls on a Sunday, then the Monday immediately thereafter shall be observed as a holiday.

The other six (6) 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

The products will be delivered to, and used at, VA locations throughout the fifty (50) states; San Juan, Puerto Rico; and/or Manila, Philippines. Incidental services required under any resulting contract(s) may be performed at any VA facility throughout these locations. A listing of specific VA locations, for informational purposes, only, may be found at http://www1.va.gov/directory/guide/home.asp?isFlash=1.

Delivery locations will be specified in any resulting, individual Delivery Orders.

4.3 TRAVEL

The Government anticipates that travel will be required for performance of various task requirements described herein. Program Management (PM) travel for Contract level tasks will not be directly reimbursed by the Government and shall be included in the Offeror's Firm Fixed Price for IT Hardware Commodity Products. PM task requirements supporting Time and Materials (T&M) efforts may be captured at the Delivery Order level. In the event that additional travel is required, these requirements and costs shall be specified and the terms negotiated at the Delivery Order level. Travel for Standard Installation and Warranty shall be captured in the Offeror's Firm Fixed Prices for Standard Installation and Warranty, respectively. For any travel in Time and Material Delivery Orders these shall be captured as Other Direct Costs (ODCs).

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor, which for purposes of this document shall encompass the prime Contractor and all subcontractors, shall perform the following tasks:

5.1 PROGRAM MANAGEMENT AND REPORTING

The Contractor shall provide program management support at the both the Contract and Delivery Order level. This Program Manager or Program Management Team shall work closely with the Government to

manage contractual and programmatic issues that arise during performance of the Contract. The Contractor PM shall be responsible for the execution of all Contract tasks to include, but not be limited to: program reviews; kickoff meetings; status updates; various reporting requirements; and day-to-day concerns.

5.1.1 CONTRACT POST AWARD CONFERENCE

The Contractor shall coordinate and administer a Contract Post Award Conference at the Contractor's facility with key stakeholders and subject matter experts (SMEs), all of whom shall be identified by the VA Office of Information Technology (OIT) Project Manager (PM). The Contractor shall schedule the Conference within ten (10) business days after contract award or as agreed upon between the VA Contracting Officer's Technical Representative (COTR), the CO, and the Contractor. At the Conference, the Contractor shall present the details of the intended approach for managing the Contract, including an Initial Draft Contract Level Work Plan and Schedule to support the quarterly Contract Level Program Review requirements described in paragraph 5.1.3 below. All the key Contractor personnel shall be present for this initial review. Side meetings shall be held to allow for further in-depth discussion of the various program areas as necessary. The Contractor shall provide Post Award Conference Meeting Minutes and an Action Item Summary electronically to the COTR and all meeting participants no later than ten (10) days after conclusion of the Contract Post Award Conference.

Deliverables:

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

5.1.2 DELIVERY ORDER KICKOFF MEETINGS

If required by the COTR and/or CO, the Contractor shall participate in kickoff meetings to be procured at the Delivery Order level. The purpose of this meeting is for the Contractor to brief the Government on how it intends to meet all the requirements of the Delivery Order. At the Government's election, the kickoff meetings may be held on-site at the Contractor's facility, Government facility, or by telephone conference. Specific requirements will be detailed in the individual Delivery Orders.

5.1.3 PROGRAM REVIEWS

The Contractor shall conduct Contract Level Program Reviews on a quarterly basis. At the Government's election, the Program Reviews may be held on-site at the Contractor's facility, Government facility, or by telephone conference. These Program Reviews shall address and provide in-depth information on program progress and all functions summarized by Delivery Order(s) to include, but not be limited to:

1. Administration
2. Schedule
3. Configuration Management
4. Technology Refresh / Insertion Products
   - Summary of tech insertion/refresh activities
   - Provide a technology roadmap identifying product lifecycle milestones, new technologies and product end-of-life (EOL) replacement strategies
5. Logistics

6. Testing
7. Quality Assurance
8. Field Support
9. Customer Issues and Resolutions

The Contractor shall provide Program Review Minutes, Action Item Summary, and an updated Contract Level Work Plan and Schedule, electronically, to the COTR and all meeting participants no later than ten (10) days after conclusion of the Contract Level Program Review.

Deliverables:

A. Program Review Minutes
B. Action Item Summary
C. Updated Contract Level Work Plan and Schedule

5.1.4 PROJECT MANAGEMENT PLAN

If required by the individual Delivery Order, the Contractor shall provide a Project Management Plan (PMP) specifying the approach, timeline, and tools to be used in execution of the Delivery Order. The PMP shall include the risk, quality and technical management approach, detailed master schedule and milestones, project change control method, and proposed personnel. The Contractor shall keep the PMP current throughout the Delivery Order period of performance. The PMP shall take the form of both a narrative and graphic format that addresses the requirements discussed above. The PMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as specified within the Delivery Order. The initial PMP shall be delivered electronically to the COTR no later than ten (10) days after award of the Delivery Order. Updates are to be provided on an as-needed basis.

Deliverables:

A. Project Management Plan and Updates

5.1.5 MONTHLY PROGRESS REPORTS

If required by the individual Delivery Order, the Contractor shall submit a Monthly Progress Report (MPR) via electronic mail. The MPRs shall address project status, including all work completed during the reporting period and work planned for the subsequent reporting period. The MPR shall also identify any problems that arose and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation. The Contractor shall monitor performance against the PMP (if applicable) and report any deviations. It is expected that the Contractor shall maintain communication with the VA so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

The Contractor shall provide the COTR with MPRs in electronic form in Microsoft Word and Project formats no later than five (5) days after the end of the preceding month. These reports shall reflect data as of the last day of the preceding month.

The MPR shall include, but not be limited to, the following items:

1. Project status and progress summary by Delivery Order
2. Summary of equipment delivered and/or installed/de-installed that month
3. Summary of repairs, including date/time/location of repair and whether repair was accomplished on-time
4. Significant open issues, risk and mitigation action
5. Summary of problems resolved
6. Subcontractor performance – discuss 1st tier subcontractors and vendor performance
7. Schedule status
8. Status of required background investigations
9. Invoices, by Contract Line Item Number (CLIN), submitted and payments received to date
10. Warranty Information
11. License Information
12. Any other areas as specifically identified by the VA as detailed in the individual Delivery Orders

Monthly reports shall not contain security related information.

Deliverables:

A. Monthly Progress Report

5.1.6 CEC ORDERING PORTAL/PRODUCT CATALOG/DELIVERY ORDER TRACKING

The Government will establish and maintain a web-based ordering portal. Ten (10) days after contract award, the Contractor shall provide the Government with CEC Ordering Portal information for all Contractor IT Hardware Commodities offered. This information shall include, but not be limited to:

1. Vendor IT Hardware Commodity Item Specification Sheet
2. Incidental Software (SW) and Hardware (HW) Dependencies
3. Manufacturer
4. Manufacturer Part Numbers
5. Unit Prices
6. Product Description

After receipt of approval from the CO, the Contractor shall provide updated information for the portal to reflect changes in products, prices, and notify and replace products reaching EOL with the newly refreshed and inserted products.

The CEC Ordering Portal will also be used as a Delivery Order Tracking System up to the point of, and including, delivery of the products. Therefore, the Contractor shall also provide up-to-date, information as necessary on the CEC Ordering Portal including, but not limited to:

1. Procurement / Delivery Date
2. Electronic Contract Management System (eCMS) Contract/ Order Number
3. Integrated Funds Distribution Control Point Activity Accounting & Procurement (IFCAP) Purchase Order Number
4. VA Delivery Site Code (if applicable)
5. VA Delivery Site Mailing Address
6. Equipment Model Listing
7. Equipment Serial Number Listing
8. Equipment Status up to and including delivery confirmation

9. Warranty Information
10. Incidental Software License Information
11. Toll Free Phone Number described in Paragraph 9.0

The CEC Ordering Portal will be used to present all IT Hardware Commodity products and incidental services offered by the CEC contract to customers as well as up-to-date status and tracking information from within a single Ordering Portal.

Where possible, the Contractor shall use electronic means to collect data to populate the portals and reduce paper (for example electronic signature pads) to validate delivery.

In addition, ten (10) days after award, the Contractor shall deliver a catalog to the COTR and CO detailing all IT Hardware Commodity products and prices offered by the Contractor in their proposal for the CEC Contract. The catalog shall also include identification of, and associated prices for, subcomponents/modules for the Servers, Networking Appliances, and Storage Arrays/Storage Appliances Technical Functional Areas. The Government reserves the right to purchase any and/or all subcomponents/modules as specified in the Contractor's catalog.

Deliverables:

A. CEC Ordering Portal Information and Updates
B. Catalog

5.1.7 CHANGE MANAGEMENT PLAN

The Contractor shall submit a Change Management Plan that details its process to manage changes to the hardware delivered under this Contract. This Plan must include all changes as described in PWS Attachment A ("Engineering Change Proposals") and describe the methods by which the Contractor validates that the hardware delivered to the Government meets the requirements of the Government's detailed specifications. These methods should include, but not be limited to, necessary performance testing procedures performed by the Contractor and/or necessary VA System Acceptance Testing described in paragraph 7.0. The Plan shall also include the methods by which the Contractor ensures all necessary hardware documentation is updated to adequately reflect these changes. The Change Management Plan shall be delivered electronically to the COTR no later than thirty (30) days after contract award. The Contractor is hereby advised that it shall not substitute hardware/equipment, or make any modifications thereto, which would result in any change to the vendor/Original Equipment Manufacturer (OEM) model or part number proposed, unless authorized, in writing, by the Contracting Officer (CO) through the Engineering Change Proposal (ECP) process.

Deliverables

A. Change Management Plan

5.1.8 TECHNOLOGY REFRESH

The Contractor shall monitor all IT Hardware Commodity products provided under this Contract and notify the CO if any products are required to be changed or updated to accommodate the latest technology. If any IT Hardware Commodity products are approaching the end of their product lifetime (EOL) (e.g., if a vendor/ OEM will no longer be marketing, selling, or promoting a particular product, or limiting or ending support for said product) the Contractor shall provide notification and an ECP, as defined in PWS

Attachment A, to the Contracting Officer Technical Representative (COTR) and CO within thirty (30) days prior to the EOL date. Notification can be either via email or overnight mail. The Contractor shall update the CEC Ordering Portal within ten (10) days (as defined in Section 5.1.6) with product refresh information, upon Government approval. The Government reserves the right to reject any Contractor-proposed ECP, at no cost to the Government.

In performing technology refreshment, the Contractor shall maintain the same brand name items as identified in the original Contract to the maximum extent practical.

The following conditions shall be met in performing a technology refresh:

a. The product(s) refreshed shall be fully compatible/backwards compatible with the originally provided product.
b. The product(s) refreshed shall meet or exceed the mandatory technical requirements as stated in the applicable specifications.
c. The product(s) refreshed shall be off-the-shelf configurations.
d. The product prices proposed, and incorporated into any resulting contract, are binding and thereby establish the Government's maximum liability for said product over the life of the Contract. Therefore, the price of the product(s) refreshed, including support services, shall not exceed the price proposed and incorporated into the basic Contract, for the product being refreshed.
e. All refreshed products shall comply with the VA Acceptance testing defined in Section 7.0 of this PWS.

Deliverables:

A. Technology Refresh Engineering Change Proposal

5.1.9 TECHNOLOGY INSERTION

As new IT Hardware technologies are developed and used by the commercial industry or the Government, the VA and/or Contractor may identify these technologies, and propose necessary additions, modifications, upgrades, enhancements, and improvements to the proposed contract IT Hardware Commodity product items. The Contractor shall translate the technology insertion recommendation into a formal ECP for the CO's approval. The Government reserves the right to reject any Contractor-proposed ECP, at no cost to the Government.

All inserted products shall undergo VA Acceptance testing as defined in Section 7.0 of this PWS.

Deliverables:

A. Technology Insertion Engineering Change Proposal

5.1.10 INCIDENTAL SOFTWARE

Stand alone purchasing of software licenses is not within the scope of this PWS. However, software licenses incidental to, and necessary for, the successful operation of IT Hardware commodities that are not a part of the VA Gold Image (as defined in Section 7.0) may be included in any resulting Delivery Orders on a Time and Materials basis. Any incidental software shall go through VA Pre-Certification and Acceptance testing and/or shall be allowed by the One-VA Technology Reference Model (www.va.gov/trm). Offerors are hereby advised that in the event of conflict between the One-VA TRM and the CEC Solicitation, the Solicitation documents take precedence.

5.1.11 INCIDENTAL HARDWARE

In order for proper installation and/or integration of IT Hardware commodities, incidental hardware may be required. These incidental hardware items may consist of, but are not limited to: subcomponents/modules; cables; cords; racks; wires; and peripherals. These items, with the exception of subcomponents/modules which shall be purchased on a Firm Fixed Price basis, will be identified in individual Delivery Orders on a Time and Materials basis and shall be directly related to hardware purchased under the CEC contract.

5.1.12 INCIDENTAL SERVICES

Services that are required for successful implementation of the IT Hardware commodities purchased may be acquired under the CEC Contract. These services shall be directly related to hardware purchased under the CEC contract vehicle. The services listed within Section 10.0 are within the scope of the Contract.

6.0 TECHNICAL FUNCTIONAL AREAS

The Contractor shall provide the following IT Hardware Commodities and all incidental hardware, software, services, and licenses to render the hardware operational. Incidental software required shall be specified in individual Delivery Orders. The Contractor shall provide all commercially available hardware documentation to include specifications, installation guides, user's manuals and/or any additional standard hardware documentation in hard copy, electronically, or both. Specific details and quantities shall be described in the individual Delivery Orders.

The Contractor shall provide only new equipment and new parts for the required products described herein. **ABSOLUTELY NO "GRAY MARKET GOODS" shall be provided under any Delivery Order.** Gray Market Goods are defined as genuine branded goods sold outside of an authorized sales-territory (or by non-authorized dealers in an authorized territory) at prices lower than being charged in authorized sales territories (or by authorized dealers).

If software is required under a Delivery Order, the Contractor shall only provide the latest commercially available version unless authorized, in writing, by the CO.

6.1 END USER DEVICES

The Contractor shall provide End User Devices to facilitate information and data processing. Detailed specifications for each configuration tier are provided in PWS Attachment B, entitled "End User Devices Specifications." Although the Government desires as minimal OEMs as possible for those products identified in the table, below (e.g., a single OEM for Laptops compatible with a Windows operating system, a single OEM for the Monitors (both Small and Large)), the Contractor may provide one (1) OEM per End User device as referenced in the below table. The Contractor shall ensure that all end user devices are delivered pre-installed with the operating system required by the applicable delivery order, as well as the VA provided Gold Image as detailed in Section 7.0, unless otherwise stipulated in the individual Delivery Orders. The Gold Image will be distributed as Government Furnished Information (GFI) as detailed in the individual Delivery Orders.

Group 1: End User Devices (PWS 6.1)	Single OEM for Light Laptop compatible with Windows OS

	Single OEM for Docking Station that is compatible with the Offeror's proposed Light Laptop Single OEM for Medium Laptop compatible with Windows OS Single OEM for Docking Station that is compatible with the Offeror's proposed Medium Laptop Single OEM for Heavy Laptop compatible with Windows OS Single OEM for Docking Station that is compatible with the Offeror's proposed Heavy Laptop Single OEM for PC – Tablet compatible with Windows OS Single OEM for Docking Station that is compatible with the Offeror's proposed PC – Tablet Single OEM for – Monitors (Small) Single OEM for – Monitors (Large) Single OEM for – Laptops compatible with Mac OS (Medium, Heavy) Single OEM for Docking Station that is compatible with the Offeror's proposed Mac OS Laptops Single OEM for – Semi-Ruggedized Laptops compatible with Windows OS Single OEM for Docking Station that is compatible with the Offeror's proposed Semi-Rugged Laptop Single OEM for – Thin Clients compatible with Windows OS Single OEM for – Desktops compatible with Mac OS

6.2 MOBILE TABLETS

The Contractor shall provide Mobile Tablets to facilitate information/data processing and computing mobility across the VA. The five (5) Mobile Tablets required span three (3) configuration tiers and therefore, must be compatible with the following: Mac OS; Android OS; and Blackberry OS. Detailed specifications for each configuration tier are provided in PWS Attachment C, entitled "Mobile Tablet Specifications."

6.3 SERVERS

The Contractor shall provide Servers to facilitate information/data processing, network services, database management and warehousing, community collaboration, training, web services, and/or resource distribution (e.g., cloud computing) across the VA. The Servers span three (3) configuration tiers: Class A, Class B, and Class C (Rack/Blade). Detailed specifications for each configuration tier and for two (2) Chassis configurations are provided in PWS Attachment D, entitled "Server Specifications." The Contractor shall provide products from a single OEM for all Class A/B/C Servers (Rack & Blade) and the two (2) Chassis configurations which meet the specification requirements.

6.4 NETWORKING APPLIANCES

The Contractor shall provide Switches and Routers to facilitate network connectivity and communication across the VA. The Switches span three (3) configuration tiers: Enterprise Class Modular LAN Campus Core Switch; Enterprise Class Stackable Network Access Switch; and Enterprise Class High Density Modular LAN Access Switch. The Routers consist of three (3) configuration Tiers: Class A; Class B; and Class C. Detailed specifications for all Switches and Routers configuration tiers are provided in PWS Attachment E, entitled "Switch Specifications," and PWS Attachment F, entitled "Router Specifications." Although the Government desires that all Networking Appliances be provided by a single OEM, the Contractor may provide Networking Appliances from more than one (1) OEM provided that each product meets the specification requirements.

6.5 STORAGE ARRAYS/STORAGE APPLIANCES

The Contractor shall provide Storage Arrays/Storage Appliances to facilitate data warehousing, management, sharing, and streaming across the VA. The Storage Arrays/Storage Appliances consist of thirteen (13) configuration tiers: Direct Attached Storage (DAS); Storage Area Network (SAN) Storage; Fibre Fabric SAN Switch; Network Attached Storage (NAS); Modular NAS Storage; Modular iSCSI Storage; LTO Tape Library; LTO Tape Cartridge; IP based Deduplication Storage; Virtual Tape Library (VTL) with Deduplication Storage; Unified Storage; Archive Storage; and GRID based Object Type Storage. Detailed specifications for each configuration tier are provided in PWS Attachment G, entitled "Storage Arrays/Storage Appliances." The Contractor shall provide products from a single OEM, per each configuration tier that meet the specification requirements up to a possible total of thirteen (13) OEM's if required.

6.6 SECURITY PLATFORMS

The Contractor shall provide security platforms to protect our Veterans personal information and protect the VA IT enterprise from cyber attacks and intrusion. The Security Platforms are comprised of three (3) products within one (1) configuration tier. Detailed specifications for the Security Platforms are provided in PWS Attachment H, entitled "Security Platform Specifications." Although the Government desires that all Security Platforms within the configuration tier be provided by a single OEM, the Contractor may provide Security Platforms from more than one (1) OEM provided that each product meets the specification requirements.

7.0 VA SYSTEM ACCEPTANCE TESTING

In addition to the requisite operating system installed on the applicable end user device, VA will create a custom operating system image that will be named "VA Gold Image" for Contractor installation. The VA Gold Image shall be provided to the Contractor as GFI, after contract award to enable orders for End User Devices. Please be advised that contractors cannot participate in Delivery Order competitions that include

requirements for End-User devices requiring Gold Images until the End-User devices have passed VA acceptance testing. Image updates and/or testing of the current image will occur if/when the Contractor introduces new equipment models to VA over the life of the contract, or if a flaw is discovered in the VA Gold Image. Any device changes that take place within any current models will also need to go through the same testing of the drivers. The Gold Image will include only applications from current/future VA enterprise licensed software. In addition, once VA builds the Gold Image it will be delivered electronically to a secure file transfer protocol (FTP) site. The Contractor shall be responsible that a FTP site is established and hosted, at the Contractor's expense. The Contractor shall store all VA images securely at its site, in accordance with VA security and policies as depicted in PWS Addendum B. If issues arise with electronic transfer of the image, VA will pursue alternative physical transfer options with the Contractor.

Within ten (10) business days of receipt of a VA Gold Image and/or as part of every engineering change proposal (e.g., a new make/model/devices within a model due to technology refresh or insertion), the Contractor shall furnish, at no cost to VA, the proposed End User Device (one of each configuration) to VA's Pre Production Test facility located in Albany, NY and/or other VA-designated location. The VA Pre-Production Test Facility will test the equipment and image to ensure that it functions correctly within the current VA IT infrastructure; regression testing must take place involving VA application software to ensure that the VA-specific hard drive image is functioning correctly. The Government will complete product testing as soon as practicable, however, this regression testing requires a minimum of thirty (30) days for completion before items can be set to ship. Upon successful regression testing, VA will notify the Contractor that the image has passed testing, and the manufacturer may begin building the end user device VA has ordered using the accepted image. This imaging shall take place on the end user device assembly line and include appropriate burn-in time to ensure image integrity. The end user device manufacturer's standard device management and diagnostic software shall be provided to VA. If the proposed equipment fails to pass the Pre-Production testing, VA will return the devices that failed to the Contractor or designated manufacturer point of contact (at the Contractor's cost), and the Contractor shall provide new devices to the pre-production testing facility. If the test unit passes, the accepted test unit will be returned to the Contractor. VA reserves the right to reject any change proposal at no cost to VA.

As part of the VA Gold imaging process, all laptop Basic Input Output System (BIOS) must be set to Preboot Execution Environment (PXE) as first boot option, and hard drive controller set to Advanced Technology Attachment (ATA) (no Redundant Array of Independent Disks (RAID) enabled). VA reserves the right to change these settings, if desired, before any required delivery. The Contractor imaging process shall support Software Change and Configuration Management (SCCM) for Operating System Deployment (OSD) OEM images including proactive driver management and driver packs that are small and optimized for SCCM OSD, specifically. The Contractor shall support multiple image file formats, the main file format the VA uses is Windows Imaging Format (wim). The Contractor shall allow for created images to be applied seamlessly to systems at the factory during the manufacturing process. Acceptance testing for all other commodities will be completed in accordance with commercially established practices, at the VA site, unless otherwise provided for in individual Delivery Orders.

8.0 STANDARD INSTALLATION (CONUS ONLY)

The Contractor may be required to provide installation support for all IT Hardware Commodities listed in the Technical Function Areas, Section 6.0, as specified in individual Delivery Orders. The Contractor shall provide the standard documentation (e.g., User Manual, Operators Manual, Installation Guide, etc.) to support the installation of the new hardware. The Contractor shall validate successful operation of any installed products prior to acceptance.

The Contractor shall develop a master delivery schedule of equipment to all sites receiving delivery of

equipment as specified in each Delivery Order. This schedule shall include, at a minimum, current status of site delivery. Schedules shall be coordinated with the local designated point of contact (POC) for installation requirements for each site identified in the Delivery Order.

The Contractor shall install new equipment as indicated in each Delivery Order which may require installation of equipment after normal business hours. After-hours installation requirements will be defined in each Delivery Order and determined by each site on an installation-by-installation basis.

The Contractor shall abide by all local VA site policies and requirements regarding equipment delivery, installation and associated personnel. The Contractor shall be responsible for coordinating all deliveries by contacting the site prior to delivery to obtain knowledge of local constraints and policies, including security requirements both for equipment and personnel.

If the new equipment replaces an existing system, the Contractor shall disconnect the existing hardware and turn it over to local Government IT Operations staff for further disposition. The Contractor shall remove all storage devices (e.g., hard drives, flash memory, etc.) from replaced systems, annotate the VA identification number (EE number) and/or serial number of the new storage device and the VA identification number (EE number) and/or serial number of the replaced storage device, create a cross reference list for signature by the Information Security Officer (ISO), and turn the hard drive over to the local Government IT Operations staff.

When proposed Delivery Orders include Standard Installation requirements, the Contractor shall perform the following installation services:

1. The Contractor shall remove all packaging and waste associated with new equipment installations and dispose of accordingly. VA encourages the Contractor to use multipacks, if available.

2. The Contractor shall provide any necessary racks, mounts, brackets, installation kits, and/or cables necessary to install the required hardware to an operational state. Any incidental hardware shall be identified in the individual Delivery Orders based upon the selected Contractor's quote or proposal. Once the new hardware is installed and connected, the hardware shall be powered on, logged onto, and tested for network connectivity. Staging areas for IT Hardware commodities to be installed are usually available at most VA sites (availability and size will vary by site). The Contractor shall coordinate site staging areas with the site delivery POC as identified in the individual Delivery Order.

3. The Contractor shall prepare an Installation Certification Sheet and have the installation certified by the designated VA site installation POC. The Contractor shall insure the VA POC certifies the installation on the same day of installation, and the Contractor must deliver the Installation Certification Sheet to the Government IT Operations POC as specified in the Delivery Order.

4. If applicable, and as defined in the individual Delivery Order, the Contractor shall input VA asset identification information into the BIOS of each Desktop and/or Laptop. The method shall include both a central factory level assignment and a local VA site assignment capability.

5. The Contractor shall apply the Contractor service tag and serial number at the factory on the exterior of the equipment. The Contractor shall provide the serial numbers for each piece of equipment to the VA site installation POC and/or COTR no later than five (5) days prior to shipment to the site. Any further requirements for the service tag will be defined at the Delivery Order level.

6. The Contractor shall provide the necessary knowledge and support for installation of the IT Hardware Commodities across the local area network (LAN), virtual private network (VPN), and/or Wide Area Network (WAN) environments.

7. The Contractor shall provide support for IT hardware installation including applicable operating systems; installation of software; monitoring and adjusting system performance; application of latest hardware/software patches, security updates and service packs; and repairs and upgrades as necessary for installation of the IT Hardware Commodity.

All standard installation performed OCONUS will be deemed a custom installation in accordance with PWS paragraph 10.2.1.

9.0 WARRANTY SUPPORT (IT HARDWARE AND INCIDENTAL SOFTWARE)

The Contractor is responsible for warranty and warranty support. The Contractor shall provide, maintain, and administer warranty support agreements for use on all IT Hardware Commodities and incidental software, and shall provide extended warranty technical support at the level required in individual Delivery Orders. The Contractor shall be the primary/initial interface between the VA and the OEMs regarding all technical support issues as well as the primary interface for all warranty information.

Upon delivery of each IT Hardware Commodity, the Contractor shall pass through the applicable OEM warranty to the Government, at no additional cost to the Government. In addition, for all IT Hardware Commodities, the Contractor shall provide VA, for a period of no less than one (1) year from acceptance of the IT Hardware Commodity to the Government (except Storage Arrays/Storage Appliances, which is no less than three (3) years), the Standard or Premium Warranty, as defined below, as part of the purchase price. This Warranty shall run concurrently with any applicable pass through OEM warranty provided. The Government reserves the right to purchase additional one (1) year increments of either the Standard or Premium Warranty Support, as an Extended Warranty, for any IT Hardware Commodity Item. The Government can purchase an Extended Warranty, be it Standard or Premium Warranty Support, for an item, as outlined in the table below, at any time prior to the expiration of the then in-effect Warranty coverage period, for that item. However, if the then in-effect Warranty expires, it cannot be renewed. In no instance, however, shall Warranty Coverage and/or Support exceed five (5) years from the date a product is purchased.

Product Group	Standard Warranty	Premium Warranty
Group 1 – End User Devices		
Group A – Laptops Windows OS*	Unit price with 1 Year Warranty	Not Applicable
	Unit price with 2 Year Warranty	Not Applicable
	Unit price with 3 Year Warranty	Not Applicable
	Unit price with 4 Year Warranty	Not Applicable
Group B – Laptop MAC OS*	Unit price with 1 Year Warranty	Not Applicable
	Unit price with 2 Year Warranty	Not Applicable
	Unit price with 3 Year Warranty	Not Applicable
	Unit price with 4 Year Warranty	Not Applicable
Group C – Thin Clients	Unit price with 1 Year Warranty	Not Applicable

Group 2 – Mobile Tablets		
Groups A through C	Unit price with 1 Year Warranty	Not Applicable
Group 3 - Servers		
Group A – Rack Mounted/Blade	Unit price with 1 Year Warranty	Unit price with 1 Year Warranty
	Unit price with 2 Year Warranty	Unit price with 2 Year Warranty
	Unit price with 3 Year Warranty	Unit price with 3 Year Warranty
	Unit price with 4 Year Warranty	Unit price with 4 Year Warranty
	Unit price with 5 Year Warranty	Unit price with 5 Year Warranty
Group 4 – Networking Appliances		
Group A – Routers/Switches	Unit price with 1 Year Warranty	Unit price with 1 Year Warranty
	Unit price with 2 Year Warranty	Unit price with 2 Year Warranty
	Unit price with 3 Year Warranty	Unit price with 3 Year Warranty
	Unit price with 4 Year Warranty	Unit price with 4 Year Warranty
	Unit price with 5 Year Warranty	Unit price with 5 Year Warranty
Group 5 – Storage Arrays/Storage Appliances		
Groups A through K	Unit price with 3 Year Warranty	Unit price with 3 Year Warranty
	Unit price with 4 Year Warranty	Unit price with 4 Year Warranty
	Unit price with 5 Year Warranty	Unit price with 5 Year Warranty
Group 6 – Security Platforms		
Group A – Security Devices	Unit price with 1 Year Warranty	Unit price with 1 Year Warranty
	Unit price with 2 Year Warranty	Unit price with 2 Year Warranty
	Unit price with 3 Year Warranty	Unit price with 3 Year Warranty
	Unit price with 4 Year Warranty	Unit price with 4 Year Warranty
	Unit price with 5 Year Warranty	Unit price with 5 Year Warranty

*Note: Standard and Premium Warranty requirements do not apply to Docking Stations. Accordingly, Offerors are not required to provide these warranties with its proposed docking stations; Offerors shall only pass-through the applicable OEM warranty.

For Storage Arrays/Storage Appliances, this Standard or Premium Warranty shall be for a period of no less than three (3) years, shall be deemed part of the purchase price, and shall run concurrently with any applicable pass through OEM warranty provided. The Government reserves the right to purchase additional one (1) year increments of either the Standard or Premium Warranty Support, as an Extended Warranty for any storage array/storage appliance. The Government can purchase an Extended Warranty, be it Standard or Premium Warranty Support, for an item at any time prior to the expiration of the then in-effect Warranty coverage period, for that item. However, if the then in-effect Warranty expires, it cannot be renewed. In no instance, however, shall Warranty Coverage and/or Support exceed five (5) years from the date a product is purchased.

For all IT Hardware Commodities, the Warranty shall begin on the first day following the date the equipment is accepted by the Government in accordance with Paragraph 12.0. The Contractor may provide third (3rd) party warranties provided that OEM original and refurbished parts, along with OEM certified technicians, are utilized by the 3rd party vendor.

Warranty Technical Support Levels

The following defines the Standard Warranty Technical Support, and where applicable, the Premium Warranty Technical Support, required for each IT Hardware Commodity Group, which the Contractor shall provide when specified in individual Delivery Order requirements.

END USER DEVICES/MOBILE TABLETS

Standard Warranty

- Technical telephone and email support shall be available Monday – Friday (i.e., standard five (5) day business week) from 9:00 am to 5:00 pm local time of the impacted VA site. The Contractor shall provide a dedicated toll-free line that will route directly to a Contractor Tier 2 or 3 customer service/technical support representative, and not a Tier 1 help desk/support technician.

- The Contractor shall acknowledge the VA's request for warranty support, via email or call-back, within two (2) business hours of receipt, in accordance with the days and times specified above.

- Contractor's initial on-site or remote diagnosis shall be completed within one (1) business day.

- Following diagnosis, on-site labor/repair and/or part/product replacement shall be completed by the Contractor within the same or next business day.

- The Contractor shall have repaired or replaced all failing equipment, to fully operational status, by Close of Business (COB) on the second business day after diagnosis. The Contractor shall bear all shipping costs for replacement parts and replacement of the product.

- Twenty-four (24) hour access to Contractor or OEM provided web support/knowledge base.

- Access to all product/firmware microcode patches, updates, and upgrades.

Premium Warranty (N/A)

SERVERS/NETWORKING APPLIANCES (SWITCHES/ROUTERS)/ STORAGE ARRAYS - STORAGE APPLIANCES/SECURITY PLATFORMS

Standard Warranty

- Technical telephone and email support shall be available Monday – Friday (i.e., standard five (5) day business week) from 9:00 am to 5:00 pm local time of the impacted VA site. The Contractor shall provide a dedicated toll-free line that will route directly to a Contractor Tier 2 or 3 customer service/technical support representative, and not a Tier 1 help desk/support technician.

- The Contractor shall acknowledge the VA's request for warranty support, via email or call-back, within two (2) business hours of receipt, in accordance with the days and times specified above.

- Contractor's initial on-site or remote diagnosis shall be completed within one (1) business day.

- Contractor's initial attempt to repair shall be completed within one (1) business day following the Contractor's initial on-site or remote diagnosis. Contractor shall provide steady efforts to ensure that the product is restored to fully operational status.

- Each additional business day that the issue is unresolved shall result in the issue continuously being escalated to the next support level, until top level support is reached. The Contractor shall provide the VA with a clear escalation time-line from the Contractor's help desk support technician to the Chief Executive Officer (CEO), or otherwise equivalent highest level Officer.

- Twenty-Four (24) hour access to Contractor or OEM web support/knowledge base.

- Access to all product/firmware/ microcode patches, updates and upgrades.

Premium Warranty

- Technical telephone support shall be available twenty-four (24) hours X seven (7) days a week X 365 days a year. The Contractor shall provide a dedicated toll-free line that will route directly to a Contractor Tier 2 or 3 customer service/technical support representative, and not a VA Tier 1 help desk/support technician.

- Tier 2 or 3 response to VA's request for warranty support shall be made within fifteen (15) minutes of VA's initial contact.

- Contractor's initial on-site or remote diagnosis shall be completed within four (4) hours.

- Contractor's initial attempt to repair shall be completed within four (4) hours following the Contractor's initial on-site or remote diagnosis. Contractor shall provide steady efforts to ensure that the product is restored to fully operational status.

- Each four (4)-hour period that the issue is unresolved shall result in the issue continuously being escalated to the next support level, until top level support is reached. The Contractor shall provide the VA with a clear escalation time-line from the Contractor's help desk support technician to the Chief Executive Officer (CEO), or otherwise equivalent highest level Officer.

- Twenty-Four (24) hour access to Contractor or OEM web support/knowledge base.

- Access to all product/firmware/ microcode patches, updates and upgrades.

Regardless of whether the Contractor is providing Standard or Premium Warranty Technical Support, the VA will provide internal Tier 1 help desk support for the IT Hardware Commodity purchased under any resulting contract. The process flow is defined in PWS Attachment I, entitled "CEC Call Flow." The Contractor shall provide a dedicated toll-free line that will route directly to a Tier 2 customer

service/technical support representative versus a Tier 1 VA help desk/support technician. If the OEM and the Contractor are not the same, the Contractor is responsible to work through the escalation process. The Contractor shall provide a clear escalation time line and process through all levels of technical support.

Under both Standard and Premium Warranty Technical Support, the Contractor shall provide asset tracking information to the VA Tier 1 Help Desk for all IT Hardware Commodities. Data to be provided shall include, at a minimum:

1. eCMS Contract/order number
2. IFCAP Purchase Order Number
3. VA Delivery Site Code if applicable
4. VA Delivery Site Mailing Address
5. Equipment Model
6. Equipment Serial Number
7. Warranty Information
8. Hardware / Software License Information

9.1 WARRANTY REPAIR

The Contractor shall provide on-site warranty repair services in accordance with the timeframes set forth in the applicable technical support level specified in an individual Delivery Order. The Contractor shall repair or replace all failing equipment covered under the warranty. In the event that failing/defective equipment capable of storing VA data (e.g., hard drives, storage devices, mobile tablets, laptops, etc.) is replaced pursuant to the Warranty, the Contractor shall disconnect and/or remove the failing/defective equipment and turn said equipment over to local Government IT Operations Staff for disposition, and/or removal of VA data where possible. If authorized by the Government, failing/defective equipment that is replaced pursuant to the Warranty and is not capable of storing VA data, or from which all VA data has successfully been removed, shall be returned to the Contractor. All replacement items shall, at a minimum, assume the remaining warranty period of the original item replaced. The Contractor shall use OEM original and refurbished parts along with OEM certified technicians to perform any warranty repair. The Contractor shall bear all shipping costs for replacement parts. The Contractor shall only maintain spare parts inventories at VA locations when explicitly approved by the Government.

If the Contractor is not the manufacturer, the Contractor shall manage the service/support function. Additionally, the Contractor is responsible for ensuring that its own or any subcontractor-provided technical support does not void a pass through OEM warranty. If Contractor/Subcontractor provided technical support results in a warranty being voided, the Contractor will still be responsible for providing warranty support with no degradation in system operational status or availability to the VA. Certified VA IT Operations staff shall be authorized to repair faulty equipment on-site without voiding warranties purchased if this is deemed most expeditious to returning the unit to service. These repair services may be conducted by VA or VA contracted staff.

As stated previously, the Contractor shall make available Standard and Premium Extended Warranty coverage for the specified IT Hardware commodities in increments of one (1) year, where applicable, but in no event shall extended warranty coverage exceed five (5) years from date of the purchase of the IT

Hardware Commodity.

The Contractor shall provide a report of all warranties to the Government as detailed in the individual Delivery Orders and provide a listing of any warranties within 180 days of expiration as an attachment to the Monthly Progress Report.

10.0 INCIDENTAL TECHNICAL SUPPORT SERVICES

The following services shall be provided by the Contractor for required support above and beyond standard installation and warranty requirements identified in Sections 8.0 and 9.0 and as specifically identified in individual Delivery Orders. These incidental services will be reimbursed on a Time and Materials basis.

10.1 PRE-DEPLOYMENT SUPPORT SERVICES

10.1.1 SITE SURVEYS

When required, the Government will provide the Contractor access to VA sites to perform site surveys necessary to develop plans for the installation/initialization of the newly acquired hardware and associated incidental software. The Contractor shall take into account floor plans and layouts, existing IT systems, existing software systems and interfaces, existing cabling, power distribution, grounding, heating, ventilating, and air conditioning (HVAC) systems, access floor systems, lighting, backboards, and any other required GFE and materials.

If facility/structural alterations are required to support installation, all such alterations must be authorized and performed by the Government.

10.2 INSTALLATION AND INITIALIZATION SUPPORT

10.2.1 CUSTOM INSTALLATION, DESIGN AND CONFIGURATION

The Contractor shall provide custom installation, design and configuration support above and beyond standard installation requirements identified in Section 8.0 and as identified in the individual Delivery Orders. These services shall include but are not limited to technical areas such as system design, de-installation, data migration, and OCONUS installations.

10.3 POST-DEPLOYMENT SUPPORT SERVICES

10.3.1 TRAINING SUPPORT

The Contractor shall provide standard commercial training and other services related to installation, set-up, configuration and use of purchased equipment.

Training requirements shall be specified in individual Delivery Orders.

10.3.2 APPLICATION SUPPORT

Application support shall include support for installation, configuration, upgrading, patching, and/or debugging of all incidental software. If the Contractor is not the software manufacturer, the Contractor shall manage the service/support function.

If a software failure is suspected, the Contractor shall attempt to resolve the issue remotely in accordance with VA security standards and policies. If the software cannot be resolved remotely, the Contractor shall arrange for an on-site technician to be dispatched to resolve the issue. The Contractor shall repair or replace all failing incidental software as required by the terms of the applicable warranty unless otherwise specified in the individual delivery order. The Contractor shall bear all shipping costs.

Application Support requirements shall be specified in individual Delivery Orders.

10.3.3 INCIDENTAL SOFTWARE LICENSES

The Contractor shall provide licenses and support for incidental software as appropriate. The Contractor shall be responsible for providing licenses as detailed in individual Delivery Orders.

The Contractor shall provide a report of all licenses provided to the Government, as specified in the individual Delivery Orders.

11.0 PACKAGING, HANDLING, STORAGE AND TRANSPORTATION

The Contractor shall establish packaging, handling, storage and transportation processes and procedures to prevent damage and mishandling of the hardware, software and incidental items from acquisition through installation. The Contractor shall be liable for all damage, deterioration, and/or losses incurred during shipment, handling, storage and transportation unless the damage, deterioration, and/or losses are due to the fault of the Government.

The Contractor shall identify and report to the Government any unique or special packaging, handling, storage or transportation requirements.

The Contractor shall be responsible for transporting equipment and personnel required for installation to the installation site. Movement of equipment from the delivery site to the staging and installation locations may require vehicles with lift capability or machine transport carts. The Contractor shall provide its staff with vehicles, carts, trash, receptacles, and any other equipment or supplies necessary to carry out the requirements of each Delivery Order. VA anticipates, at a minimum, that carts will be required at all sites. Additional site requirements will be provided during pre-installation coordination with the sites and as specified in the individual Delivery Orders.

Unless otherwise specified, all items shall be preserved, packaged, and packed in accordance with standard commercial practices and in a manner that will afford protection against corrosion, deterioration and physical damage during shipment. The items shall be packed in a manner which conforms to the requirements of Uniform Freight Classification for rail shipment, National Motor Freight Classification for truck shipment, Parcel Post Regulations, and the regulations of other carriers as applicable to the mode of transportation employed.

Exterior shipping containers and items not shipped in containers shall be clearly marked on an external surface as follows:

a) Delivery Point of Contact (POC) & Phone number
b) Contract Number
c) Delivery Order Number
d) IFCAP Purchase Order Number
e) Itemized list of contents including quantity and Contract Line Item Number (CLIN)

12.0 VA DELIVERY ACCEPTANCE

Each Delivery Order issued will have its own Acceptance Official. Unless otherwise specified within a Delivery Order, acceptance of all items delivered under the CEC Contract will take place at the VA site specified on each individual Delivery Order. The Contractor shall only tender for acceptance those items that conform to the requirements of the CEC Contract and Delivery Order under which delivery of IT Hardware Commodities are required. VA may request equipment be delivered to an individual facility without having the Contractor install the equipment. In these instances, VA will take responsibility for the equipment at the delivery location and free the Contractor from all responsibilities associated with initial equipment installation. In these instances, the date of acceptance shall be considered to be the date of equipment delivery.

13.0 GENERAL REQUIREMENTS

13.1 ENTERPRISE AND IT FRAMEWORK

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (One-VA TRM). One-VA TRM is one (1) component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the IT used to develop, operate, and maintain enterprise applications. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. Architecture, Strategy, and Design (ASD) has overall responsibility for the One-VA TRM.

As required and defined in the individual delivery orders the Contractor shall support VA efforts in accordance with the Program Management Accountability System (PMAS) 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, PMAS is a VA-wide initiative to better empower the OI&T Project Managers and teams to meet their mission: delivering world-class IT products that meet business needs on time and within budget.

ProPath is a VA-wide process management tool that builds upon the OI&T Program and Development managers' delivery of high-quality products, and provides an 'at-a-glance' perspective of nearly every step in the software development process. If applicable to the individual delivery order the Contractor shall utilize the tools and templates, and shall file documents in ProPath as a central resource as required by the VA PMAS Process.

13.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

The following security requirement must be adhered to regarding Contractor owned equipment used to support the VA. 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 the 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 COTR, CO, the PM, and the ISO must be notified and verify all security requirements have been adhered to.

1. Information made available to the Contractor/Subcontractor by VA for the performance or

administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, Federal Acquisition Regulation (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 shall 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 are in compliance with VA directive requirements.
3. Prior to termination or completion of this contract, Contractor/Subcontractor shall not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by the 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 shall be sent to the VA CO within thirty (30) days of termination of the Contract.
4. The Contractor/Subcontractor shall 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 for cause under Federal Acquisition Regulation (FAR) Part 12.
7. The Contractor/Subcontractor shall 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.

8. 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.
9. 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 shall refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA CO for response.
10. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA CO for response.
11. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require Certification and Accreditation (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 COTR.
12. Position Sensitivity and Background Investigation - The position sensitivity and the level of background investigation commensurate with the required level of access is:

☐ Low/NACI
☐ Moderate/MB
☒ High/BI

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	**Minimum 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, spouse, neighbors, supervisor, co-workers; 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; and a verification of the educational degree.

Contractor Responsibilities:

a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language. The Contractor shall provide the name, address, date of birth, Social Security Number and any other pertinent and relevant information of the Contractor personnel assigned to this project to the COTR and CO, as requested, and prior to the Delivery Order Level Kickoff Meetings.

b. The Contractor shall bear the expense of obtaining background investigations. If the investigation is conducted by the Office of Personnel Management (OPM), the Contractor shall reimburse VA within thirty (30) days.

c. The Contractor(s) and Contractor point of contact (POC) will receive an email notification from the Security and Investigation Center (SIC) identifying the website link that includes detailed instructions regarding completion of the background clearance application process and what level of background clearance was requested. Reminder notifications will be sent if the complete package is not submitted by the due date.

d. The Contractor shall submit or have their personnel submit the required forms (SF 85P - Questionnaire for Public Trust Positions, SF 85P-S – Supplemental Questionnaire for Selected Positions, FD 258 – U.S. Department of Justice Fingerprint Applicant Chart, VA Form 0710 – Authority for Release of Information Form, Optional Form 306 – Declaration for Federal Employment, and Optional Form 612 – Optional Application for Federal Employment) to the VA Office of Security and Law Enforcement within thirty (30) calendar days of receipt.

e. All costs associated with obtaining clearances for Contractor provided personnel shall be the responsibility of the Contractor. Further, the Contractor shall be responsible for the actions of all individuals 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.

f. If the security clearance investigation is not completed prior to the start date of the contract, the contract employee may work on the Contract with an initiated status while the security

clearance is being processed. However, the Contractor shall be responsible for the actions of the Contractor personnel it provides to perform work for the VA. In the event damage arises from work performed by Contractor personnel, under the auspices of the contract, the Contractor shall be responsible for resources necessary to remedy the incident.

g. The investigative history for Contractor personnel working under this Contract must be maintained in the databases of either the OPM or the Defense Industrial Security Clearance Organization (DISCO).

h. The Contractor, when notified of an unfavorable determination by the Government, shall withdraw the employee from consideration in working under the contract.

i. Failure to comply with the Contractor personnel security requirements may result in termination of the contract for default.

13.3 METHOD AND DISTRIBUTION OF DELIVERABLES

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

13.4 PERFORMANCE METRICS

The Contractor shall monitor performance against the established schedule, milestones, risks and resource support outlined in the approved PMP. The Contractor shall report any deviations in the Monthly Progress Report. As a minimum, the following metrics shall be included*:*

Performance Objective	Performance Standard	Acceptable Performance Levels	Surveillance Method
1. Technical Needs	Shows understanding of requirements Efficient and effective in meeting requirements Meets technical needs and mission requirements Offers quality services/products	Achieve 3.0 or higher	Performance Assessment
2. Project Milestones and Schedule	Quick response capability Products completed, reviewed, delivered in timely manner Notifies customer in advance of potential problems	Achieve 3.0 or higher	Performance Assessment
3. Project Staffing	Currency of expertise Personnel possess necessary knowledge, skills and abilities to	Achieve 3.0 or higher	Performance Assessment

	perform tasks		
4. Value Added	Provided valuable service to Government Services/products delivered were of desired quality	Achieve 3.0 or higher	Performance Assessment

Detailed Performance Metrics shall be identified in the individual Delivery Orders.

The contractor shall comply with IEEE 1680 "Standard for Environmental Assessment of Personal Computer Products"—also known as the Electronic Product Environmental Assessment Tool (EPEAT)—the first U.S. standard that provides guidelines for identifying environmentally friendly desktop and laptop computers and monitors. For more detailed information on the EPEAT criteria, visit http://www.epeat.net/. All End- User Devices (PWS section 6.1) provided under this contract, with the exception of docking stations, shall be rated EPEAT "Silver" or higher. Equipment provided on this contract is required to comply with EPA disposal standards.

The Government will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the support required by this PWS in an acceptable manner. The Government reserves the right to alter or change the QASP at its own discretion. A Performance Based Service Assessment Survey will be used in combination with the QASP to assist the Government in determining acceptable performance levels.

13.5 FACILITY/RESOURCE PROVISIONS

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

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

The VA shall provide access to VA specific systems/network as required for execution of the task via a site-to-site VPN or other technology, including VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath, Primavera, and Remedy, including appropriate seat management and user licenses. The Contractor shall utilize government-provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort. The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall In Accordance With (IAW) VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. For detailed Security and Privacy Requirements refer to ADDENDUM A and ADDENDUM B.

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.[1] The Contractor's firewall and web server shall meet or exceed the VA minimum requirements for security. All VA data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer as soon as possible. The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to certification and accreditation.

Each documented initiative under this contract incorporates the security clause VAAR 852.273-75 by reference as though fully set forth therein, as well as the VA Handbook 6500.6, "Contract Security," March 12, 2010, in its entirety. Both the security clause VAAR 852.273-75 and 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 at https://www.ees-learning.net/librix/loginhtml.asp?v=librix.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)

[1] See VAAR 852.273-75 referenced *infra*.

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 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 the 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 the 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 the VA.
7. Contractor must adhere to the following:
8. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
9. Controlled access to system and security software and documentation.
10. Recording, monitoring, and control of passwords and privileges.
11. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
12. 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.
13. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
14. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
15. Contractor does not require access to classified data.
16. 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

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

1. 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 Delivery Order.
2. 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.
3. 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.
4. 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.
5. 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 the VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in

Rights in Data - General, FAR 52.227-14(d) (1).

2. 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 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 the 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 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 an 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 COTR.

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 COTR, and approved by the VA Privacy Service in accordance with Directive 6507, *VA Privacy Impact Assessment*.
2. The Contractor/Subcontractor shall certify to the COTR 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 the 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 the VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes based upon the requirements identified within their contract.

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

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

1. 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 COTR 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.
2. 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.
3. 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.
4. 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, Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

5. 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 COTR. 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.
6. 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, 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.
7. 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 the 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.
8. 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:
    a. Vendor must accept the system without the drive;
    b. 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
    c. VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.
    d. Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for the VA to retain the hard drive, then;

        i. 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

        ii. 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.

        iii. 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

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

2. 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.

3. 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.

4. 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

1. 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.

2. 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.

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

    a. Nature of the event (loss, theft, unauthorized access);
    b. Description of the event, including:
        i. date of occurrence;
        ii. data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
    c. Number of individuals affected or potentially affected;
    d. Names of individuals or groups affected or potentially affected;
    e. 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;
    f. Amount of time the data has been out of VA control;
    g. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
    h. Known misuses of data containing sensitive personal information, if any;
    i. Assessment of the potential harm to the affected individuals;
    j. Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and
    k. 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.

4. 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:

    a. Notification;
    b. One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
    c. Data breach analysis;
    d. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
    e. One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
    f. 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

1. 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:

    a. 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;
    b. Successfully complete the *VA Cyber Security Awareness and Rules of Behavior* training and annually complete required security training;
    c. Successfully complete the appropriate VA privacy training and annually complete required privacy training; and
    d. Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access

2. The Contractor shall provide to the contracting officer and/or the COTR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

3. 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.