|  |
| --- |
| VeteransAffairs-Seal.JPG  |

**PERFORMANCE WORK STATEMENT (PWS)**

**DEPARTMENT OF VETERANS AFFAIRS**

**Office of Information & Technology**

**Enterprise Operations (EO)**

**Storage on Demand**

**Date: Jan 17, 2014**

**PWS Version Number: 4.6**

Contents

[1.0 BACKGROUND 5](#_Toc379530467)

[2.0 APPLICABLE DOCUMENTS 5](#_Toc379530468)

[3.0 SCOPE OF WORK 7](#_Toc379530469)

[4.0 PERFORMANCE DETAILS 7](#_Toc379530470)

[4.1 PERFORMANCE PERIOD 7](#_Toc379530471)

[4.2 PLACE OF PERFORMANCE 8](#_Toc379530472)

[4.3 TRAVEL 8](#_Toc379530473)

[4.4 TYPE OF AGREEMENT AND ORDER 8](#_Toc379530474)

[4.5 SPECIFIC TASKS AND DELIVERABLES 9](#_Toc379530475)

[4.6 CONTRACT MANAGEMENT 9](#_Toc379530476)

[4.6.1 CONTRACTOR PROGRAM MANAGEMENT 9](#_Toc379530477)

[4.6.2 CONTRACTING PROJECT MANAGEMENT PLAN 9](#_Toc379530478)

[4.6.3 WEEKLY TELECONFERENCE 9](#_Toc379530479)

[4.6.4 WEEKLY ORDER SUMMARY 9](#_Toc379530480)

[4.6.5 PROGRESS REPORTS 10](#_Toc379530481)

[4.6.6 ADDITIONAL MEETINGS/TELECONFERENCES 10](#_Toc379530482)

[4.6.7 KICKOFF MEETING 10](#_Toc379530483)

[4.6.8 SEMI-ANNUAL REVIEW MEETINGS 10](#_Toc379530484)

[4.7 CONTRACT REQUIRED PERIODIC REPORTING REQUIREMENTS 11](#_Toc379530485)

[4.7.1 CONTRACTOR’S PROGRESS, STATUS AND MANAGEMENT REPORT 11](#_Toc379530486)

[4.7.2 MONTHLY INVENTORY REPORT 12](#_Toc379530487)

[4.7.3 MONTHLY INCIDENT SUMMARY 12](#_Toc379530488)

[4.7.4 MONTHLY CAPACITY AND BILLING REPORTS 12](#_Toc379530489)

[4.7.5 QUARTERLY INVENTORY REPORT 12](#_Toc379530490)

[4.7.6 QUARTERLY INCIDENT SUMMARY 12](#_Toc379530491)

[4.7.7 QUARTELY CAPACITY AND BILLING REPORTS 13](#_Toc379530492)

[4.7.8 AD HOC REPORTS 13](#_Toc379530493)

[5.0 PERFORMANCE REQUIREMENTS 13](#_Toc379530494)

[5.1 STORAGE SOLUTIONS AND CAPABILITIES 13](#_Toc379530495)

[5.1.1 SUPPORTIVE ENVIRONMENTS 13](#_Toc379530496)

[5.1.2 ENTERPRISE CLASS STORAGE SOLUTIONS (HIGH PERFORMANCE) 14](#_Toc379530497)

[5.1.3 ENTERPRISE CLASS STORAGE (MID-PERFORMANCE) SOLUTIONS 15](#_Toc379530498)

[5.1.4 ENTERPRISE CLASS STORAGE (LOW-PERFORMANCE) SOLUTIONS - INEXPENSIVE BULK STORAGE DISK SOLUTIONS 16](#_Toc379530499)

[5.1.5 NAS STORAGE-HIGH PERFORMANCE 16](#_Toc379530500)

[5.1.6 NAS STORAGE-MEDIUM PERFORMANCE 17](#_Toc379530501)

[5.1.7 NAS STORAGE-LOW PERFORMANCE 17](#_Toc379530502)

[5.1.8 BIG DATA, OBJECT-ADDRESSABLE STORAGE SOLUTION - GRID BASED OBJECT EXTRA LARGE STORAGE 17](#_Toc379530503)

[5.1.9 BIG DATA, OBJECT-ADDRESSABLE STORAGE SOLUTION - GRID BASED OBJECT (LARGE) 18](#_Toc379530504)

[5.1.10 BIG DATA, OBJECT-ADDRESSABLE STORAGE SOLUTION - GRID BASED OBJECT (MEDIUM) 18](#_Toc379530505)

[5.1.11 DATA DE-DUPLICATION CAPABILITIES - IP BASED DEDUPE – XLARGE 18](#_Toc379530506)

[5.1.12 DATA DE-DUPLICATION CAPABILITIES - IP BASED DEDUPE – LARGE 18](#_Toc379530507)

[5.1.13 VIRTUAL TAPE LIBRARY (VTL) CAPABILITIES – XLARGE 18](#_Toc379530508)

[5.1.14 VIRTUAL TAPE LIBRARY (VTL) CAPABILITIES – LARGE 18](#_Toc379530509)

[5.1.15 VIRTUAL TAPE LIBRARY (VTL) CAPABILITIES – MEDIUM 18](#_Toc379530510)

[5.1.16 LARGE-FIBRE FABRIC SAN SWITCH 19](#_Toc379530511)

[5.2 STORAGE SERVICES 19](#_Toc379530512)

[5.2.1 ARCHITECTURE DESIGN AND CONFIGURATION 19](#_Toc379530513)

[5.2.2 MANAGEMENT SERVICES 19](#_Toc379530514)

[5.2.3 RACK AND POWER REQUIREMENTS 21](#_Toc379530515)

[5.2.4 POWER FEED AND INTERFACES 21](#_Toc379530516)

[5.2.5 RACK REQUIREMENTS 21](#_Toc379530517)

[5.2.6 SITE SURVEYS 21](#_Toc379530518)

[5.2.7 AVAILABILITY 21](#_Toc379530519)

[5.2.8 COMPLIANCE WITH OEM BEST PRACTICES 21](#_Toc379530520)

[5.3 PROVISIONING, MANAGEMENT AND REPORTING INFRASTRUCTURE 22](#_Toc379530521)

[5.3.1 DIAGNOSTIC, HARDWARE, VIRTUALIZATION, PERFORMANCE 22](#_Toc379530522)

[5.3.2 STORAGE RESOURCE MANAGEMENT (SRM) SOLUTION 22](#_Toc379530523)

[5.3.3 STORAGE REPORTING & CHARGEBACK 23](#_Toc379530524)

[5.3.4 CONFIGURATION AND ASSET MANAGEMENT 23](#_Toc379530525)

[5.3.5 CENTRAL MANAGEMENT INTERFACE 23](#_Toc379530526)

[5.3.6 STORAGE RESOURCE MANAGEMENT (SRM) INTEGRATION 24](#_Toc379530527)

[5.4 MAINTENANCE 24](#_Toc379530528)

[5.4.1 MAINTENANCE RESPONSE AND REPAIR TIME 24](#_Toc379530529)

[5.4.2 MAINTENANCE TYPES 25](#_Toc379530530)

[5.5 COMPLIANCE WITH INDUSTRY IT PRINCIPLE BEST PRACTICE STANDARDS 27](#_Toc379530531)

[5.5.1 CHANGE MANAGEMENT 27](#_Toc379530532)

[5.5.2 CONFIGURATION MANAGEMENT 27](#_Toc379530533)

[5.5.3 ASSET MANAGEMENT 27](#_Toc379530534)

[5.5.4 RELEASE MANAGEMENT 28](#_Toc379530535)

[5.5.5 PERFORMANCE MONITORING AND REPORTING 28](#_Toc379530536)

[5.5.6 CAPACITY MANAGEMENT 28](#_Toc379530537)

[5.6 SERVICE TRANSITION STRATEGY 28](#_Toc379530538)

[5.6.1 TRANSITION IN STRATEGY 28](#_Toc379530539)

[5.6.2 TRANSITION EXIT STRATEGY 29](#_Toc379530540)

[5.7 DELIVERY, INSTALLATION, CONFIGURATION, AND REMOVAL SUPPORT 29](#_Toc379530541)

[5.7.1 DELIVERY OF STORAGE SOLUTION 29](#_Toc379530542)

[5.7.2 INSTALLATION, DE-INSTALLATION, AND POWER-UP CONFIGURATION 29](#_Toc379530543)

[5.7.3 REMOVAL OF EQUIPMENT 29](#_Toc379530544)

[5.7.4 TECHNICAL DOCUMENTATION 29](#_Toc379530545)

[5.7.5 TEST NEW STORAGE TECHNOLOGIES 30](#_Toc379530546)

[5.7.6 TRAINING 30](#_Toc379530547)

[5.8 TECHNICAL ASSISTANCE AND CONSULTING SUPPORT 30](#_Toc379530548)

[5.9 TECH REFRESH. 30](#_Toc379530549)

[5.9.1 REFRESH VALIDATION 31](#_Toc379530550)

[6.0 GENERAL REQUIREMENTS 31](#_Toc379530551)

[6.1 ENTERPRISE AND IT FRAMEWORK 31](#_Toc379530552)

[6.2 POSITION/TASK RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS 32](#_Toc379530553)

[6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S) 32](#_Toc379530554)

[6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS 33](#_Toc379530555)

[6.3 METHOD AND DISTRIBUTION OF DELIVERABLES 35](#_Toc379530556)

[6.4 PERFORMANCE METRICS 35](#_Toc379530557)

[6.5 FACILITY/RESOURCE PROVISIONS 35](#_Toc379530558)

[6.6 GOVERNMENT FURNISHED PROPERTY 36](#_Toc379530559)

[6.6.1 Government-Furnished Equipment (GFE)/Government-Furnished Information (GFI). 36](#_Toc379530560)

[6.6.2 Configuration and Customization Rights and Non-Disclosure Agreement. 37](#_Toc379530561)

[ADDENDUM A 38](#_Toc379530562)

# BACKGROUND

The mission of the Department of Veterans Affairs (VA) Enterprise Operations (EO) is to provide high quality, cost-effective information technology (IT) business solutions to VA and other Federal agency customers. EO has been a major data center in VA’s system for over 40 years and is committed to supporting the Department’s IT requirements.

EO provides Data Protection services to its customers’ data through disk mirroring and tape backups. Routine evaluation of the tape and storage environment is required to ensure Data Protection and Disaster Recovery resources are available to the customer in a timely manner. To meet its customers’ ever increasing data storage requirements it has to maintain a large amount of storage. Maintaining large volumes of un-used storage for any given period of time is not cost effective, increasing the storage costs to our Corporate Data Center Operations (CDCO) customers, and is becoming extremely challenging with such technologies as cloud computing.

VA requires a storage approach that is tailored to the storage demands of the EO customer and not only takes into account growth, but also the rate of growth and the predictability or unpredictability of that growth. Such an approach needs to be scalable to address the various performance needs of the EO customer as well as capacity.

A ‘storage on demand’ strategy, sometimes referred to as “Utility Computing”, would enable the datacenters to position large amounts of storage platforms (fully populated) on the computer room floor and only be charged when utilized (on demand). This approach aligns operational needs with procurement; reduces capital expenditures; provides ready-for-use capacity in as little as 72 hours; and possibly could negate maintenance costs. The VA EO is the owner, as there will be extra capacity on the floor to meet on demand requests. This capacity management is required for each of the sites listed in place of performance.

A storage on demand strategy coupled with Management Services will provide EO with a holistic storage service offering in a timely manner.

# APPLICABLE DOCUMENTS

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

1. 44 U.S.C. § 3541, “Federal Information Security Management Act (FISMA) of 2002”
2. Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements For Cryptographic Modules”
3. FIPS Pub 201, “Personal Identity Verification of Federal Employees and Contractors,” March 2006
4. 10 U.S.C. § 2224, "Defense Information Assurance Program"
5. Software Engineering Institute, Software Acquisition Capability Maturity Modeling (SA CMM) Level 2 procedures and processes
6. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
7. **42 U.S.C. § 2000d “**Title VI of the Civil Rights Act of 1964”
8. Department of Veterans Affairs (VA) Directive 0710, “Personnel Suitability and Security Program,” May 18, 2007
9. VA Directive 6102, “Internet/Intranet Services,” July 15, 2008
10. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
11. OMB Circular A-130, “Management of Federal Information Resources,” November 28, 2000
12. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
13. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
14. 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
15. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
16. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, , 2012
17. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” September 20, 2012
18. VA Handbook 6500.1, “Electronic Media Sanitization,” March 22, 2010
19. VA Handbook 6500.2, “Management of Data Breaches Involving Sensitive Personal Information (SPI)”, January 6, 2012
20. VA Handbook 6500.3, “Certification and Accreditation of VA Information Systems,” November 24, 2008
21. VA Handbook, 6500.5, “Incorporating Security and Privacy in System Development Lifecycle” March 22, 2010
22. VA Handbook 6500.6, “Contract Security,” March 12, 2010
23. Project Management Accountability System (PMAS) portal (reference PWS References -Technical Library at <https://www.voa.va.gov/>)
24. OIT ProPath Process Methodology (reference PWS References -Technical Library and ProPath Library links at <https://www.voa.va.gov/>) NOTE: In the event of a conflict, OIT ProPath takes precedence over other processes or methodologies.
25. Technical Reference Model (TRM) (reference at <https://www.voa.va.gov/>)
26. National Institute Standards and Technology (NIST) Special Publications

VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008

VA Directive 6300, Records and Information Management, February 26, 2009

VA Handbook, 6300.1, Records Management Procedures, March 24, 2010

OMB Memorandum, “Transition to IPv6”, September 28, 2010

TRM Storage Requirements – (Attachment 1)

Telecommunications Industry Association (TIA) 942 - Telecommunications Infrastructure Standards for Data Centers

[ITIL](http://searchdatacenter.techtarget.com/definition/ITIL) - Information Technology Infrastructure Library

ITSM ISO 20000 – Information Technology Service Management

# SCOPE OF WORK

The Contractor shall provide on-demand storage solutions to include designing, delivering, installing, and maintaining storage capacity infrastructure at the current VA EO computing facilities (refer to Section 4.2). The Contractor may also be required to provide on-demand storage solutions to future VA EO computing facilities. The Contractor shall provide storage management services to operate, augment and maintain the on-demand storage solutions. In providing storage management services, the Contractor is expected to cover all functional areas to include, but not limited to, design capabilities, systems engineering, hardware, software, software maintenance, licensing, logistical support, and field maintenance.

This PWS provides general requirements. Specific requirements shall be defined in individual orders. Individual order requirements may fall within one specific task, but in many cases, the requirements will encompass and apply across multiple tasks. Individual orders will delineate reporting requirements as detailed in section 4.7.

The Contractor may be required to perform some or all the tasks indentified in this Performance Work Statement as specified in individual orders.

# PERFORMANCE DETAILS

## PERFORMANCE PERIOD

The ordering period for this effort is expected to be 60 months.

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

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

Under current definitions, four are set by date:

New Year's Day January 1

Independence Day July 4

Veterans Day November 11

Christmas Day December 25

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

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

Martin Luther King's Birthday Third Monday in January

Washington's Birthday Third Monday in February

Memorial Day Last Monday in May

Labor Day First Monday in September

Columbus Day Second Monday in October

Thanksgiving Fourth Thursday in November

## PLACE OF PERFORMANCE

Tasks under this PWS shall be performed at any of the five existing VA EO data centers and future VA EO data centers which may be stood up in any of the 48 contiguous states. VA EO existing data centers are listed below:

Austin Information Technology Center (AITC)

1615 Woodward Street (200/313)
Austin, Texas 78772

Hines Information Technology Center (HITC)

1st Ave. N. of 22nd St., Bldg #215
Hines, IL 60141

Philadelphia Information Technology Center (PITC)

5000 Wissahickon Avenue

Philadelphia, PA  19144

Capital Region Readiness Center (CRRC)

221 Butler Avenue, Bldg. 511

Martinsburg, WV 25405

Quantico Information Technology Center (QITC)

18424 Joplin Road (Route 619)
Triangle, VA 22172

## TRAVEL

Travel shall be in accordance with individual order requirements. The amount of travel and locations will be specified in the individual orders. In a Firm Fixed Price (FFP) order, travel costs shall be amortized across the line item prices.

## TYPE OF AGREEMENT AND ORDER

To Be Determined.

## SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

## CONTRACT MANAGEMENT

### CONTRACTOR PROGRAM MANAGEMENT

The Contractor shall establish a single management focal point, the Program/Project Manager, to accomplish the administrative, managerial and financial aspects of all orders. This individual shall be identified to the Contracting Officer’s Representative (COR) and CO as the focal point for all programmatic issues.

### CONTRACTING PROJECT MANAGEMENT PLAN

The Contractor shall deliver a Contractor Project Management Plan (CPMP) that lays out the Contractor’s approach, timeline and tools to be used in execution of the contract.  The CPMP should take the form of a narrative and graphic format that displays the schedule (to include a Host Migration Schedule), milestones, risks and resource support.  The CPMP shall also describe how the Contractor will coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The initial baseline CPMP shall be concurred upon and updated monthly thereafter. The Contractor shall update and maintain the VA PM approved CPMP throughout the period of performance.

### WEEKLY TELECONFERENCE

The Contractor shall conduct weekly status teleconference meetings to discuss completed and outstanding tasks, project challenges as well as order status and installation/repair status. The weekly time will be established by the Government during normal weekday business hours. The Government is the only party that has the unilateral right to cancel or change a teleconference.

### WEEKLY ORDER SUMMARY

The Contractor shall provide Weekly Order Summary Reports. Each report shall include (but is not limited to) the following: Order number, order received, valid order date, order line number, CLIN, SLIN, description, customer, project, quantity, delivery location, make, model, VA EO requestor, technical POC, base price, extended price, VA EO billing information (Resource Pools, Customer Code (MCC), Application Code (APPL), etc.), estimated ship date, actual ship date, estimated delivery date, actual delivery, estimated install date, actual install, actual provision date, acceptance date, order status, and description.

### PROGRESS REPORTS

The Contractor shall provide the COR with Weekly Progress Reports in electronic form in Microsoft Office software such as Word, Project.  Each report shall include detailed instructions/explanations for each required data element, to ensure that data is accurate and consistent. Each report shall reflect data as of the last day of the preceding Week.

The Weekly Progress Reports shall cover all work completed during the reporting period and work planned for the subsequent reporting period.  Each report 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 including their plan and timeframe for resolving the issue. The Contractor shall monitor performance against the CPMP and report any deviations. It is expected that the Contractor will keep in communication with VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

### ADDITIONAL MEETINGS/TELECONFERENCES

The Contractor is expected to participate in additional meetings and teleconferences as part of their standard work week. These additional meetings and teleconferences may be required based on issues that need to be addressed. The time will be mutually agreed upon. The Contractor shall provide meeting minutes after each meeting.

### KICKOFF MEETING

The Contractor may be required to conduct a one day Kickoff meeting within 10 calendar days after each individual order is awarded. The Kickoff meeting shall take place virtually or at the location specified by the individual order. In the Kickoff meeting the Contractor shall present the CPMP to include the details of its intended approach, work plan and project schedule including deliverable dates for review and approval by the Government. The Kickoff meeting shall include an implementation review; perform validation of sites current configuration, review the business and IT requirements, goals, expectations, and success parameters associated with the engagement. The Contractor shall provide meeting materials and meeting minutes to include action items resulting from the Kick-Off meeting.

### SEMI-ANNUAL REVIEW MEETINGS

The Government and the Contractor will have semi-annual contract meetings. The meeting site and forum will be determined by the VA EO program manager. The meeting will be held to review contract status. The Government is the only party that has the unilateral right to cancel or change a meeting. The Contractor shall provide meeting agenda and meeting materials for each meeting. The Contractor shall prepare a report summarizing the meeting within five workdays after completion.

## CONTRACT REQUIRED PERIODIC REPORTING REQUIREMENTS

The Contractor shall be required to provide the following reports on the 5th workday of the month.

### CONTRACTOR’S PROGRESS, STATUS AND MANAGEMENT REPORT

The Contractor shall submit a Monthly Status Report. Orders that are completed shall be listed as such.

1. For each Order, indicate/discuss the following:
2. Order summary
3. Performance metrics
4. Order schedule
5. PMAS Compliancy (as applicable)
6. Critical items for Government review
7. Accomplishments
8. Significant open issues, risk and mitigation action
9. Summary of issues closed
10. Meetings completed
11. Projected meetings
12. Subcontractor performance – discuss 1st tier Subcontractors and vendor performance
13. Projected activities for next reporting period
14. Explanation if the reporting period is over one month
15. For each Fixed Price Task indicate the following:
16. Receiving report submitted
17. Milestone payment schedule
18. For each T&M Task, indicate the following:
19. High level summary
20. Expenditures for the reporting period
21. Subcontract Line Item Number (SLIN) expenditure
22. Burn rate
23. Percentage of work completed

1. General and Cumulative Performance. Indicate the following:
2. Any general meetings that occurred with Government representatives during the reporting period
3. Total dollars awarded to date (ceiling)
4. Total dollars invoiced to date, by fiscal year, and since BPA award. These figures shall be further broken out by dollars and percentage of time and materials invoices vs. fixed price invoices.

### MONTHLY INVENTORY REPORT

The Contractor shall provide Monthly Inventory Reports. Each report shall include, but is not limited to, the following: contract number, order numbers, hardware makes and models, serial numbers, configuration components (cabinets, disk numbers, sizes and speeds, ports, slots, transports, etc.), total capacity allocated and billing, microcode versions, physical locations (to include: site location, floor tile location, etc.), environment order dates, installation dates, and acceptance dates.

### MONTHLY INCIDENT SUMMARY

The Contractor shall provide Monthly Incident Summary Reports. Each report shall include, but is not limited to, the following: description of incident, hardware makes and models, serial numbers, physical locations, (to include: site location, floor tile location, etc.), environment date and time of incident, date and time of resolution, summary of action taken to resolve.

### MONTHLY CAPACITY AND BILLING REPORTS

The Contractor shall provide Monthly Capacity and Billing Reports. Each report shall include, but is not limited to, the following: site (location), total raw storage, total usable, total allocated (presented to the array and host), and total storage used (consumed) by the host.

* Host information is needed at the virtual as well as physical server layer
* All consumption values will be in Gigabytes
* The report must be exportable to EXCEL for further analysis by the VA EO Business Office personnel
* Clustered servers are only accounted for once not on a per server basis

### QUARTERLY INVENTORY REPORT

The Contractor shall provide Quarterly the Monthly Inventory Reports rolled up in an operations review. Each report shall include but is not limited to the following: contract number, order numbers, hardware makes and models, serial numbers, configuration components (cabinets, disk numbers, sizes and speeds, ports, slots, transports, etc.), total capacity allocated and billing, microcode versions, physical locations (to include: site location, floor tile location, etc.), environment order dates, installation dates, and acceptance dates.

### QUARTERLY INCIDENT SUMMARY

The Contractor shall provide Quarterly the Monthly Incident Summary Reports rolled up into an operations review. Each report shall include but is not limited to the following: description of incident, hardware makes and models, serial numbers, physical locations, (to include: site location, floor tile location, etc.), environment date and time of incident, date and time of resolution, summary of action taken to resolve. Assess that best practices are in use

### QUARTELY CAPACITY AND BILLING REPORTS

The Contractor shall provide Quarterly the Monthly Capacity and Billing Reports rolled up into an operations review. Each report shall include but is not limited to the following: site (location), total raw storage, total usable, total allocated (presented to the array and host), and total storage used (consumed) by the host.

* Host information is needed at the virtual as well as physical server layer
* All consumption values will be in Gigabytes
* The report must be exportable to EXCEL for further analysis by the VA EO Business Office personnel
* Clustered servers are only accounted for once not on a per server basis

### AD HOC REPORTS

The Contractor shall provide Ad Hoc Reports. These Ad Hoc reports will be assigned on an as required basis which is based upon Government emergent requirements.

# PERFORMANCE REQUIREMENTS

##  STORAGE SOLUTIONS AND CAPABILITIES

The Contractor shall provide a flexible, highly scalable, on-demand solution(s) that are non-disruptive and support a multi-tier storage environment. The Contractor’s solution(s) shall identify the storage protocols, including but not limited to, iSCSI, Infiniband, Fibre Channel over Ethernet (FCoE). The on-demand solution(s) shall meet the different class storage requirements identified in Sections 5.1.2 thru 5.1.16 below.

### SUPPORTIVE ENVIRONMENTS

#### MULTI-TENANT ENVIRONMENT

The Contractor shall provide storage solutions that support multi-tenancy within a multi-client architecture. Multi-tenancy is defined as the ability to utilize the same solution for multiple client systems, while providing the same level of service to all workloads accessing the solution.

#### SERVERS

The Contractor shall provide Storage solutions that support the following server chipsets/operation environments for VA EO facilities. In the event of chipsets/environments not being listed below the Contractor shall notify the PM of their findings. The Contractor shall submit an engineering change proposal to cover any future platforms not identified in this listing.

* IBM System z (IBM z/OS, IBM z/VM, Red Hat Enterprise zLinux, SUSE Linux Enterprise Server)
* X-86 (Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Solaris, VMware vSphere Enterprise Plus)
* Itanium (HP-UX, OpenVMS)
* SPARC (Solaris)
* IBM System P-Series (AIX)

#### STORAGE AREA NETWORK (SAN)

The Contractor shall provide solutions that are interoperable and compatible with the currently installed VA EO SAN, see Attachment 2 – Current Storage Inventory. The Contractor, when deemed necessary, shall perform site surveys to ensure performance is maintained. The Contractor shall provide interoperability metrics of compatibility with EO VA switches as identified in Attachment 2. The Contractor shall be responsible for ensuring interoperability and compatibility of any VA EO identified devices.

#### CONNECTIVITY

The Contractor shall provide SAN solutions that support common industry storage networking protocols such as Fiber Channel (FC) and Ethernet as well as fiber connectivity (FICON). The Contractor shall provide solutions for storage switching requirements priced on a per port basis.

The current environment is FC. The Offeror’s solution must support the current environment and should be flexible to include other storage networking protocols like FCoE and iSCSI.

### ENTERPRISE CLASS STORAGE SOLUTIONS (HIGH PERFORMANCE)

For external controller based redundant array of independent disks (RAID) solutions, the Contractor shall meet all of the following criteria and all the criteria listed in Attachment 1 - TRM-Storage Requirements (“Enterprise Storage-High Perf” TAB):

* Use multi-controller architecture
* Support 1TB of cache
* Support controller cache mirroring
* Support heterogeneous data migration which is non-disruptive to ongoing operations
* Support 32,000 Logical Unit Numbers (LUNs)
* Support active / active controllers with symmetric access to LUNs
* Support multi-site replication
* Support mainframe (z/OS, z/VM, and z/Linux) and open system architectures
* Support FICON and FC host connectivity
* Support synchronous data replication internal to the array, point-in-time and snap shot copies
* Support snapshots capability to remote storage systems
* Support space recovery reclamation
* Support advanced RAID capabilities (RAID 10, 5, (3+1), 5 (7+1) etc.)
* Support multi-tenancy; the ability to utilize the same solution for multiple client systems, while providing the same level of service to all workloads accessing the solution
* Perform equivalent to a Serial Attached SCSI (SAS) 15K rpm hard drive or better
* Support thin provisioning virtualization of storage resources to attached servers (This includes the ability to create multiple common storage “pools” and presenting logical storage capacity to a server while minimizing the physical storage resources consumed and allows for non-disruptive scaling (up and down) and reconfigurations)
* Support asynchronous data replication
* Support synchronous data replication external to the array
* Support automated multi-tiered life cycle management architecture that is configurable / tunable and has flexibility in its data protection options
* Support data erasure / shredding compliant with NIST FIPS 140-2
* Support Encryption of data at rest that complies with all levels of the FIPS 140-2 standard
* Enable non-disruptive migration of the data from the currently installed VA EO storage solution (see Attachment 2, Current Storage Inventory and refer to PWS Section 5.9 for Service Transition and Transition Strategy) to the proposed storage solution

All of these requirements identified above and the requirements identified in Attachment 1 are mandatory and shall be included in all enterprise storage solutions.

### ENTERPRISE CLASS STORAGE (MID-PERFORMANCE) SOLUTIONS

For mid-performance external controller based RAID solutions the Contractor shall meet all of the following criteria and criteria listed in Attachment 1 - TRM-Storage Requirements (“Enterprise Storage-Med. Perf” TAB):

* Use dual controller or cluster architecture
* Support UNIX, Windows, VMware, Linux operating systems
* Support FC host connectivity
* Support advanced RAID capabilities (RAID 10, 5 (3+1), 5 (7+1) etc.)
* Support multi-tenancy; the ability to utilize the same solution for multiple client systems, while providing the same level of service to all workloads accessing the solution
* Support controller cache mirroring
* Provide a performance equivalent to a SAS 15k rpm hard drive or better
* Virtualization of storage resources to attached servers
* Support asynchronous data replication
* Support synchronous data replication external to the array
* Support data erasure / shredding compliant with NIST FIPS 140-2
* Support synchronous data replication, point-in-time and snap shot copies
* Support Encryption of data at rest that complies with all levels of the FIPS 140-2 standard
* Enable non-disruptive migration of the data from the currently installed VA EO storage solution (see Attachment 2, Current Storage Inventory and refer to PWS Section 5.9 for Service Transition and Transition Strategy) to the proposed storage solution
* Includes a common storage “pool” and presenting logical storage capacity to a server while minimizing the physical storage resources consumed and allows for non-disruptive scaling (up and down) and reconfigurations.

### ENTERPRISE CLASS STORAGE (LOW-PERFORMANCE) SOLUTIONS - INEXPENSIVE BULK STORAGE DISK SOLUTIONS

For inexpensive, scalable, external controller based storage system, the Contractor shall meet the following criteria and criteria listed in Attachment 1 - TRM-Storage Requirements (“Enterprise Storage-Low Perf” TAB):

* Provide basic RAID capabilities (RAID 0, 1, 5),
* Use single or dual controller architecture,
* Support Virtualization of storage resources to attached servers.
* Support FICON and FC host connectivity,
* Enable non-disruptive migration of the data from the currently installed VA EO storage solution to the proposed storage contracted solution. (See Attachment 2, Current Storage Inventory and reference section 5.9 Transition Strategy)
* Includes a common storage “pool” and presenting logical storage capacity to a server while minimizing the physical storage resources consumed.

### NAS STORAGE-HIGH PERFORMANCE

For NAS high performance storage solutions, the Contractor shall meet all of the following criteria and the criteria listed in Attachment 1 - TRM-Storage Requirements (“NAS Storage-High Perf” TAB):

* Support UNIX, Windows, VMware, Linux operating systems
* Support advanced RAID capabilities (RAID 10, 5 (3+1), 5 (7+1) etc.)
* Support multiple VLANs and multi-tenancy; the ability to utilize the same solution for multiple client systems, while providing the same level of service to all workloads accessing the solution
* Support asynchronous data replication
* Support synchronous data replication, point-in-time and snap shot copies
* Support data erasure / shredding compliant with NIST FIPS 140-2, and
* Provide Encryption of data at rest that complies with all levels of the FIPS 140-2 standard
* Enable non-disruptive migration of the data from the currently installed VA EO storage solution (see Attachment 2, Storage Inventory and refer to PWS Section 5.9 for Service Transition and Transition Strategy) to the proposed storage solution

### NAS STORAGE-MEDIUM PERFORMANCE

For NAS medium performance storage solutions, the Contractor shall meet all the criteria listed in Attachment 1 - TRM-Storage Requirements (“NAS Storage-Med Perf” TAB).

### NAS STORAGE-LOW PERFORMANCE

#### For NAS low performance storage solutions, the Contractor shall meet all the criteria listed in Attachment 1 - TRM-Storage Requirements (“NAS Storage-Low Perf” TAB).

### BIG DATA, OBJECT-ADDRESSABLE STORAGE SOLUTION - GRID BASED OBJECT EXTRA LARGE STORAGE

The Contractor shall provide a solution for Big Data, Object-Addressable Storage for Extra large scale data storage. The big data, object-addressable storage solution shall be optimized for extra large scale file and unstructured data and have non-disruptive scale out capabilities. This solution shall support petabytes of unstructured data under a single name space.

Big data solutions shall meet all of the following criteria and criteria listed in Attachment 1 - TRM-Storage Requirements (“GRID Object (Extra Large)” TAB).

* Support UNIX, Windows, VMware, Linux operating systems
* Support asynchronous data replication
* Support a distributed file system capable of working across multiple, globally distributed nodes
* Support a minimum of 15 PB global name space / file system
* Support for NFS, CIFS, REST, and additional HTTP, HTTPS, FTP, FTPS SFTP, API
* Support multi-tenancy;the ability to utilize the same solution for multiple client systems, while providing the same level of service to all workloads accessing the solution
* Support a minimum of 8 gigabit, fiber Ethernet connects
* Allows for non-disruptive scaling (up and down) and reconfigurations
* Enable non-disruptive migration of the data from the currently installed VA EO storage solution (see Attachment 2, Storage Inventory and refer to PWS Section 5.9 for Service Transition and Transition Strategy) to the proposed storage solution

### BIG DATA, OBJECT-ADDRESSABLE STORAGE SOLUTION - GRID BASED OBJECT (LARGE)

The Contractor shall provide a solution for Big Data, Object-Addressable Storage for large scale data storage. The big data, object-addressable storage solution shall be optimized for large scale file and unstructured data and have non-disruptive scale out capabilities. Big data solutions shall meet all of the above criteria and criteria listed in Attachment 1 - TRM-Storage Requirements (“GRID Object (Large)” TAB).

### BIG DATA, OBJECT-ADDRESSABLE STORAGE SOLUTION - GRID BASED OBJECT (MEDIUM)

The Contractor shall provide a solution for Big Data, Object-Addressable Storage for medium scale data storage. The big data, object-addressable storage solution shall be optimized for medium scale file and unstructured data and have non-disruptive scale out capabilities. Big data solutions shall meet all of the above criteria and criteria listed in Attachment 1 - TRM-Storage Requirements (“GRID Object (Medium)” TAB).

### DATA DE-DUPLICATION CAPABILITIES - IP BASED DEDUPE – XLARGE

The Contractor shall provide storage solutions that include data de-duplication capabilities which support data replication, are scalable up and down and minimize downtime.The data de-duplication solutions shall meet all the criteria listed in Attachment 1 - TRM-Storage Requirements (“IP Based DeDupe - XLarge” TAB).

### DATA DE-DUPLICATION CAPABILITIES - IP BASED DEDUPE – LARGE

The Contractor shall provide storage solutions that include data de-duplication capabilities which support data replication, are scalable up and down and minimize downtime.The data de-duplication solutions shall meet all the criteria listed in Attachment 1 - TRM-Storage Requirements (“IP Based DeDupe - Large” TAB).

### VIRTUAL TAPE LIBRARY (VTL) CAPABILITIES – XLARGE

The Contractor shall provide storage solutions that include VTL capabilities and shall meet all of the criteria listed in Attachment 1 - TRM-Storage Requirements (“VTL – XLarge” TAB).

### VIRTUAL TAPE LIBRARY (VTL) CAPABILITIES – LARGE

The Contractor shall provide storage solutions that include VTL capabilities and shall meet all of the criteria listed in Attachment 1 - TRM-Storage Requirements (“VTL – Large” TAB).

### VIRTUAL TAPE LIBRARY (VTL) CAPABILITIES – MEDIUM

The Contractor shall provide storage solutions that include VTL capabilities and shall meet all of the criteria listed in Attachment 1 - TRM-Storage Requirements (“VTL – Med” TAB).

### LARGE-FIBRE FABRIC SAN SWITCH

The Contractor shall provide storage solutions that include Large-Fibre Fabric SAN Switch capabilities and shall meet all of the criteria listed in Attachment 1 - TRM-Storage Requirements (“Large-Fibre Fabric SAN Switch” TAB).

## STORAGE SERVICES

### ARCHITECTURE DESIGN AND CONFIGURATION

The Contractor shall as part of providing the on-demand storage solution be required to design and propose an architected solution and keep the solution design current. The architecture design shall serve as a baseline for operations and maintenance. The Contractor shall participate in the quarterly review section 4.7.5 to 4.7.7 with the VA Program Manager to review the solutions and compare against product vendor’s current best practices to ensure viability in the solutions. The design documentation shall be maintained on a VA EO provided central repository. The design documentation will serve as baselines for change controls, knowledge management, incident trouble shooting, datacenter capacity planning, and be maintained and updated in accordance to VA EO change processes. The Contractor shall gather information from these the quarterly reviews to support the current business needs.

### MANAGEMENT SERVICES

The Contractor shall provide solutions that can accommodate the following management services based on each sites’ individual storage and support needs. The Contractor shall refer to Attachment 3 (Enterprise Storage Management RACI Chart.pdf), which shows the various management services responsibility assignments matrix. RACI stands for Responsible, Accountable, Consulted and Informed. The Contractor shall provide:

* + A remote support to VA with allocation of equipment onsite
	+ A remote support to VA with allocation of equipment onsite, VA presentation of storage, and a remote consulting team
	+ A remote support to VA with allocation of equipment onsite, Shared VA storage presentation system, with onsite consultants and an onsite account manager

#### CONTRACTOR MANAGED SERVICES

The Contractor shall install, configure and manage the storage infrastructure to VA specification of Enterprise Storage Management RACI (refer to Attachment 3 - Enterprise Storage Management RACI Chart.pdf), which shows the Contractor Managed Services responsibility assignments matrix to include the provisioning of the storage.  The Contractor shall perform a site audit to assess the facilities capabilities to support the solution.

The Contractor shall submit changes to the Government and obtain approval prior to making any changes to VA environments. These changes shall be tracked and managed using the VA change management tool through appropriate VA approved connectors.

The Contractor shall ensure 24/7 coverage at all sites.

#### SHARED SERVICES

For shared services, the Contractor shall install, configure and manage the storage along with VA Data Center personnel to support VA customers. The distinction between roles and responsibilities for the Contractor and VA personnel are identified in Attachment 3 (Enterprise Storage Management RACI Chart.pdf), which shows the Shared Services responsibility assignments matrix. The Contractor shall also supplement the existing VA EO storage administration staff within the Capacity solution product line, with staff who possess a demonstrated and validated proficiency, or with a vendor supplied, certified storage administrator(s) to ensure 24/7 coverage at all sites. The additional personnel required shall be proposed by the Contractor based on the Contractor solution’s manning requirement minus the existing VA EO staffing at each location. (See Attachment 4, Current VA EO Staffing).

The Contractor shall submit changes to the Government and obtain approval prior to making any changes to VA environments. These changes shall be tracked and managed using the VA change management tool.

The Contractor shall provide tools, technology and process training leveraging a 90 day vendor supported evaluation of future storage systems to the existing VA EO system staff. (Reference PWS Section 5.7.3 Training)

#### GOVERNMENT MANAGED SERVICES

For Government Managed Services the Contractor shall install, maintain, and configure the storage to support VA customers. The Roles and Responsibilities between Contractor and VA personnel are identified in Attachment 3 (Enterprise Storage Management RACI Chart.pdf), which shows the Government Managed Services responsibility assignments matrix. The Contractor shall also supplement the existing storage administrator staff with certified storage administrators to ensure 24/7 coverage at all sites. The additional personnel required shall be proposed by the Contractor based on the Contractor solution’s manning requirement minus the existing staffing at each location (See Attachment 4, Current VA EO Staffing).

The Contractor shall provide Training to the existing VA EO system staff. (Reference PWS Section 5.7.3 Training)

### RACK AND POWER REQUIREMENTS

As part of each storage solution, the Contractor shall provide all required ancillary components (such as cables, power cables, etc.) to make each storage solution operational at each facility. The Contractor is responsible for all ancillary components up to the facility power feed and service interfaces.

### POWER FEED AND INTERFACES

The Contractor shall provide storage solutions that support the following existing power feeds (See Attachment 5 – Power Feeds and Specifications).

### RACK REQUIREMENTS

All storage solution equipment shall be installed by the Contractor using existing Racks and each installation shall meet the unique site requirements. In addition, all racks shall meet the VA Standard Rack Specifications provided in Attachment 5, which provides additional specific requirements for each site IAW with Telecommunications Industry Association (TIA) 942.

### SITE SURVEYS

The Contractor shall perform the following site related activities prior to installation taking place.

1. Notification of survey. This notification request shall be provided to the site POC at least five business days prior to requested date of access.
2. Conduct site surveys at each existing datacenter targeted for a solution.
3. Review the site’s capability document for information on existing capability.
4. Assess and review the site for power and cooling cross connects and interconnects.
5. Report and obtain Government approval of post site survey report.
6. After site survey approval, the Contractor shall develop a site equipment configuration guide, and provide a detailed electrical connection diagram for each location.

### AVAILABILITY

The Contractor shall provide storage solutions that are highly available minimum of 99.999% for enterprise class storage (High Performance) and 99.95% for all other orderable storage systems and readily scalable to adjust to increases and decreases in required storage capability and prevent data loss in the event of component failure(s). The Contractor shall provide Technical Specifications which describe how the provided solutions meet the availability and scalability storage capability. See Attachment 6, SLA

### COMPLIANCE WITH OEM BEST PRACTICES

The Contractor shall operate and maintain the storage solution in accordance with Original Equipment Manufacturer’s (OEM) specifications and recommended best practices when performing configurations of solutions. The Contractor shall include recommendations to VA EO personnel on how to achieve optimal performance of their solution(s). When exercising OEM best practices, the Contractor shall design and implement techniques (such as disk mirroring, tape backups, disaster recovery) to protect VA EO data.

## PROVISIONING, MANAGEMENT AND REPORTING INFRASTRUCTURE

### DIAGNOSTIC, HARDWARE, VIRTUALIZATION, PERFORMANCE

The Contractor shall provide a centralized management infrastructure solution to include provisioning capabilities, hardware diagnostics, hardware monitoring, virtualization management, event logging, performance management or additional back office processes required to reside in the EO infrastructure to support the Contractor’s technical solution. This solution shall manage both the Contractor’s storage solution and VA’s storage infrastructure. The centralized management infrastructure solution shall be required to scale in a way that will support VA EO storage environment and provide customizable, detailed reporting of infrastructure performance. The centralized management infrastructure solution shall be managed and maintained by the Contractor and ensure VA personnel have access. The Solution shall integrate and interoperate with existing VA Computer Associates (CA) Service Desk Management Solutions to support availability requirements.

The provided solution shall facilitate and be capable of both local and remote (via a wide area dedicated VA EO management network) centralized management. This includes operational control, performance and monitoring for storage and SAN switching networks. The Solution shall be required to send error and performance alerts to VA EO storage personnel. The Solution shall provide role-based access control to limit access. See Attachment 6, SLA

### STORAGE RESOURCE MANAGEMENT (SRM) SOLUTION

The Contractor shall provide a single integrated SRM solution that fully supports all storage services provided under this effort. The solution shall be capable of running in the VA EO environment meeting the Information Security requirements identified in VA Handbook 6500. The Contractor shall provide documentation to obtain VA EO Authority to Operate (ATO) certification. The SRM solution is required to be TRM approved ready for implementation within 45 calendar days after contract performance start. This solution shall be subject to VA EO (ATO) accreditation processes. The Contractor shall provide their Subject Matter Expertise on their solution when supporting the PM during unannounced audits, surveys and self-assessments as required by VA’s Continuous Readiness in Information Security Program (CRISP) program. The solution shall be a simple, easy to use and maintain system that has reporting which is flexible, detailed, and has maximum out of the box capabilities. The Contractor shall provide VA Storage Administrators the ability to close the procurement and fulfillment request from a technically delivered perspective back to the Provisioning system. The system shall integrate with the Computer Associates (CA) Service Delivery Management system for Change controls. See Attachment 7 for ATO Procedures.

### STORAGE REPORTING & CHARGEBACK

The SRM solution shall provide both reports and files ready for importing into MS Office compatible, or Excel spreadsheet for detailing storage utilization in Gigabytes for capacity utilization as well as financial billing purposes.

The storage reports required are as follows:

1. Enterprise wide storage reporting of all array’s storage by tier and replication status.
2. Array reporting that attributes storage to customer Physical Servers and EO Virtualization Platform Servers by tier and replication status.
3. Guest server reporting detailing storage allocated to virtualized customer servers on EO Virtualization Platforms by tier and replication status.
4. Chargeback Capability.
5. Uses Configuration Management Database extract to associate Master Customer Codes and Applications with the storage that it has attributed to each Physical and Guest server.
6. Totals the storage for each application by tier and application status.
7. Computes charges by applying the appropriate Tier and Replication rates.
8. Produces file ready for chargeback staff post processing that includes perorations and whether the storage is sustaining or new.

###### Deliverables:

1. Enterprise Wide Storage Reports
2. Array Reports
3. Guest Server Reports
4. Chargeback Capability Files

###  CONFIGURATION AND ASSET MANAGEMENT

The SRM solution shall provide Configuration and asset management information for tracking current configuration details and identify which components of a solution are in use and which are not in use.

###  CENTRAL MANAGEMENT INTERFACE

The SRM solution shall provide a central management interface for the control and management of the solution components and needs to provide:

* A SRM suite that compliments the functionality and features of the existing software suite. (See Attachment 2, Current Storage Software Inventory)
* Central Management training as required please refer to section 5.7.3
* An accredited management infrastructure solution with the ability to manage provided storage infrastructure either locally or remotely and provide centralized reporting via solution.
* A comprehensive comparison checklist between the new and existing SRM solutions features and functionality,
* A detailed migration plan outlining the steps needed to move the data to the new storage solution. The migration must coincide with the existing warranty expiration dates.
* Comprehensive comparison checklist between the new and existing SRM solutions features and functionality.

###  STORAGE RESOURCE MANAGEMENT (SRM) INTEGRATION

The Contractor shall provide a SRM solution that can integrate with VA EO implementation of CA Service Desk Manager Software Information Technology Service Management (ITSM) system.

## MAINTENANCE

The Contractor shall perform all maintenance actions as required by the OEM and identified herein to achieve system availability identified in Section 5.2.7.

### MAINTENANCE RESPONSE AND REPAIR TIME

The Contractor shall provide storage capacity that delivers a minimum of 99.999% availability for Enterprise class storage (High Performance) and 99.95% for all other orderable systems. Response and repair times shall be 2 hour response/4 hour restore, unless otherwise specified by VA EO. The Contractor shall ensure these response times do not change the requirement for 99.95 or 99.999% availability, but represent requirements to repair components which might be causing a degraded state. The Contractor shall provide detailed plans on how they will address solution failures of redundant components which might not impact system availability, but do create performance issues or introduce single points of failure in systems.

###### The Contractor shall provide 24x7/365 problem escalation/resolution support for hardware, software, and capacity management. The Contractor shall provide a multi-level solution for response after being notified by the Government, to commence remedial maintenance for hardware and any software required for the Contractor solution to operate. Each orderable system will be identified to a level of response based on Government need. All costs associated with maintenance requirements shall be included in the “utility” pricing.

### MAINTENANCE TYPES

#### PREDICTIVE MAINTENANCE

The Contractor shall monitor equipment/component performance using remote diagnostics mechanisms referenced in paragraph 5.4.2.4 for the purpose of identifying whether equipment is operating in accordance with established specifications. This includes hardware, software and any other components required to make the vendor solution operable. The Contractor shall, upon determining equipment/component is about to fail or is operating outside OEM specifications, initiate action to effect repair even though no call for remedial maintenance has been initiated by the site help desk or shift supervisor.

The Contractor shall call the managing site service desk or shift supervisor to inform them they are coming in for predictive maintenance and request a VA EO Security Services Form 200-00E-26 be generated and coordinated with the physical site. Upon arrival at the physical site, the contractor’s technician shall report to the site help desk or shift supervisor in order to comply with reporting requirements.

#### REMEDIAL MAINTENANCE

Maintenance calls will be initiated by the site help desk or shift supervisor to the Contractor’s toll free help desk service. The Contractor shall respond and repair, or when necessary, obtain required OEM support, in accordance with the equipment OEM specification. The Contractor shall complete remedial maintenance within the response and repair times required to meet the availability minimums defined in paragraph 5.4.1. Upon arrival on site, contractor’s technician shall report to the site help desk or shift supervisor in order to comply with reporting requirements. This includes hardware, software and any other components required to make the Contractor solution operable. The Contractor shall maintain a certified list of approved contractors reviewed quarterly against performance criteria.

#### PREVENTATIVE MAINTENANCE

The Contractor is responsible to schedule preventive maintenance at each facility. Preventative maintenance shall be scheduled as agreed to by the managing site POC, local site support and the Contractor. This includes preventative maintenance for hardware, software and any other components required to make the Contractor solution operable. The Contractor shall submit in writing its preventive maintenance schedule for equipment to the COR within 30 days after contract award. Submission of the schedule shall be in accordance with contractor format. The preventive maintenance schedule may be modified at no cost to the Government by mutual agreement of the parties. The Contractor’s proposed schedule shall not be less than that recommended by the OEM and shall include, as a minimum, the following information:

* Nomenclature of hardware/software/another other component item
* Model
* Serial Number
* Remote diagnostics and reporting capabilities
* Frequency and duration of preventive maintenance, and type of service to be performed

The Contractor shall commence preventative maintenance in accordance with the approved preventative maintenance schedule within 30 days after award for all maintenance equipment. Preventative maintenance shall be scheduled outside of the normal business hours.

If during the course of preventative maintenance, an equipment malfunction is identified, the Contractor shall report the malfunction to the site POC. The malfunction shall be corrected as a Remedial Maintenance Service (see paragraph 5.4.2.2) and comply with response times (see paragraph 5.4.1).

#### REMOTE DIAGNOSTICS

The Contractor shall immediately report permanent recorded system errors to remote service centers. This includes errors to hardware, software and any other components required to make the Contractor solution operable. The Contractor shall provide written confirmation that reports and remote diagnostics support for applicable equipment exist within seven calendar days after contract performance start. Storage systems shall support built in diagnostics with “phone home” type capabilities using Hypertext Transfer Protocol Secure (HTTPS), Secure File Transfer Program (SFTP), Simple Mail Transfer Protocol (SMTP), or Secure Shell (SSH) protocols.

Verbal contact between the local Government maintenance technician and an off-site Contractor support technician is not acceptable for remote diagnostics. There shall be a Contractor supplied diagnostic system usable by the remote technician.

The dial-in feature can be used, but ONLY with site authorization. The feature shall be capable of VA EO disabling and set up to provide the site the ability to enable the feature upon request from the Contractor.

#### AFTER HOURS, WEEKEND AND HOLIDAYS SUPPORT

Under certain conditions, the Contractor may be required to be available on “stand by” after hours, weekends, and/or holidays. All “stand by” hours will be included in the technical assistance and consulting support pricing. “Stand by” includes having a field engineer available on-site during a facility power upgrade.

## COMPLIANCE WITH INDUSTRY IT PRINCIPLE BEST PRACTICE STANDARDS

The Contractor shall comply with the following Information Technology Infrastructure Library (ITIL) principles or ITSM ISO 20000:

* Change Management,
* Configuration Management,
* Asset Management,
* Release Management.
* Performance Monitoring and Reporting
* Capacity Monitoring and Reporting

These industry standards will improve overall management of VA EO storage infrastructure. Companies and Government agencies that have followed the methodologies of these models have improved their service and reliability of their infrastructure reducing their long-term costs.

### CHANGE MANAGEMENT

The Contractor shall follow an established ITIL Change Management process for handling all changes to the storage infrastructure. The Contractor shall develop and provide, for review by Government, the change management plan for acceptance and approval. Over the period of performance of this contract storage technologies will change, software will be revised, and hardware will be phased out by the manufacturer. By having a process in place to handle these inevitable events, time and money can be saved. It will also be necessary to incorporate VA EO customer requests for new or revised functionality. Changes in focus and/or mission of some or all the VA EO business processes will play a role in the type of changes that may need to be incorporated into Tech Refresh Program over a five year span. This will specifically address end of life and unsupportable issues which may occur during the life of this contract.

### CONFIGURATION MANAGEMENT

The Contractor shall document and follow an established ITIL Configuration Management process for managing the infrastructure’s storage configuration. The Contractor shall provide monthly configuration/asset summary reports for configuration/asset validation by the Government.

### ASSET MANAGEMENT

The Contractor shall document and follow an established ITIL Asset Management process for handling asset returns and redeployment.

### RELEASE MANAGEMENT

The Contractor shall document and follow an established ITIL Release Management process for performing package releases to the infrastructure. Release Management works to ensure strong Configuration Management and Change Management, and works alongside Asset Management to ensure that any assets are introduced into the infrastructure correctly and with the minimum of difficulty. Release management will integrate with VA EO SDM suite processes and Pro Path workflows.

The Contractor shall coordinate with the Government storage engineering staff regarding the release and implementation of all microcode and software releases to ensure compatibility of all components. The Government develops standard documentation on version levels for all its sites in line with change and configuration management programs. All releases must be coordinated with the Government storage engineering staff prior to implementation.

### PERFORMANCE MONITORING AND REPORTING

The Contractor shall perform monitoring and reporting and must align with the VA EO monitoring systems and capabilities. The Monitoring and Reporting reports shall provide a monthly run rate of performance metrics to show point in time health and proactively manage issues. The Quarterly business reports must be reconciled with the incident reports and metrics to provide sufficient information for the business office to take appropriate action for budget and process issues or requirements.

### CAPACITY MANAGEMENT

The Contractor shall provide provisioning and capacity reports for success failure tracking on requests. Each Capacity report shall be delivered on monthly basis with a quarterly review roll up to allow the business office to plan and manage the capacity demands with the Contractor.  Each report shall be reconciled with the asset management and receiving reports for regular updates to meet the yearly budget true up and manage the cost to Government.

## SERVICE TRANSITION STRATEGY

### TRANSITION IN STRATEGY

The Contractor shall provide a detailed non-disruptive migration strategy for transitioning data from the current storage inventory to their proposed solution. The migration strategy shall provide for completing the transition of all data to the proposed Contractor’s solutions. The migration plan shall address how the Contractor will minimize the impact to current storage operations and data replication. The Contractor shall be required to meet with the Government within 45 days of issuance of the order to plan the transition strategy. The Contractor shall provide a written migration plan within 60 days of award.

### TRANSITION EXIT STRATEGY

The Contractor shall provide methodologies for transitioning the provided information storage service components to VA EO or another Contractor at the end of the contract period. At the end of the contract, or canceling of the contract, the Contractor shall be responsible for the removal of all their owned equipment (less hard drives and other types of data storage medias) related to this contract to the Government. The CO/COR may require the awarded Contractor to support EO’s future transition to a new Contractor solution upon termination or contract expiration.

## DELIVERY, INSTALLATION, CONFIGURATION, AND REMOVAL SUPPORT

### DELIVERY OF STORAGE SOLUTION

The Contractor shall provide storage solution components necessary to support contract requirements. The Contractor shall acquire, install, uninstall, transport, provide the necessary hardware maintenance, associated support software required for the Contractor solution to operate, and services to support the storage infrastructure associated with the contract. Normal equipment installations should be accomplished during regular dayshift working hours (0600-1800 local time), Monday through Friday. Under certain conditions, the Contractor may be required to perform an installation/update after normal duty hours during evenings and weekends. Although the Government will try to minimize this requirement, the Contractor must plan to work after hours, weekends, and or holidays for delivery and installation of new or updated orders. All installation requirements should be included in the “utility” pricing.

### INSTALLATION, DE-INSTALLATION, AND POWER-UP CONFIGURATION

All installation, de-installation, and power-up configuration will be completed by the Contractor based upon Government approval. The Government will perform final configuration as required.

### REMOVAL OF EQUIPMENT

The Contractor shall conduct any necessary de-installation and removal of hardware items on this contract upon request by the Government both during and at the end of the contract. Removal of all contractor equipment will be coordinated with the site Accountable Property Custodian (APC) or Property management group.

### TECHNICAL DOCUMENTATION

The Contractor shall provide current technical documentation for all provided equipment of the storage solutions.The Contractor shall define the Methodology for providing VA EO personnel with access to technical documentation for all capacity services provided in the Contractor’s offerings and “utility” pricing.

### TEST NEW STORAGE TECHNOLOGIES

The Contractor shall provide a strategy for allowing VA EO to test new storage technologies on a limited time basis at one or more of its designated locations. The testing will be conducted for determination of adding the technology to the contract and/or determination of the optimum strategy for deployment in the VA data centers. The Contractor shall provide a means for Government personnel to test and validate the proposed contracted solution.

### TRAINING

In the event the Contractor implements a storage solution unfamiliar to VA EO staff, the Contractor might be called upon to develop and provide training of the storage solution. The target audience for the training may include, but is not limited to, VA EO Storage Administrators, however the specifics will be delineated in each order. The Contractor shall conduct the training at the VA EO facilities identified in each order. A typical classroom training shall consist of hands-on training and anticipated to last 3-5 days. The training dates will be provided to the Contractor by the COR at least 10 days prior to the start of training. The Contractor shall provide:

* A high-level session designed to inform/educate other EO and National Service Desk (NSD) personnel about the new capabilities, reports, etc.
* A Path for virtualization training
* A Collaborative onsite training
* An Onsite training with a Training Plan that covers the use and functionality of all products associated with the new storage resource management suite
* An inclusion of training for unlimited staff to have access to training during the period of performance of new solutions

## TECHNICAL ASSISTANCE AND CONSULTING SUPPORT

The Contractor shall provide technical assistance and consulting support required to meet the needs of VA EO and its customers. Technical Assistance and Consulting Support is a specified requirement needed by VA EO and does not include predictive, remedial, or preventative maintenance for hardware, software, racks, or release management. The Contractor shall be responsible for providing technical assistance support and consulting support in the design and delivery of technology solutions designed to meet the Government’s business needs.

## TECH REFRESH.

On occasion the Government may have a requirement to introduce new/revised IT products which shall require the Contractor to respond in a sufficiently fast turn-around time, such as a 15 to 45 day period, to meet Government mission requirements. Consequently, the Contractor must be able to expeditiously respond to requests to accomplish any changes and must be able to specify a response time relevant to accomplishing any Government requested change to a product line.

Potential Technical Refresh Scenarios:

* Obsolescence or midyear deployment at contract onset
* Change in requirements
* Incorporated or acquired data center with aged equipment

### REFRESH VALIDATION

The Contractor has one business day to validate an order for accuracy. Once the Contractor validates an order for accuracy, the hardware should be delivered within 30 days. Orders received on Fridays require validation by the following business day.

# GENERAL REQUIREMENTS

## ENTERPRISE AND IT FRAMEWORK

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

**6.1.2** The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directives issued by the Office of Management and Budget (OMB) on August 2, 2005 (<http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf>) and September 28, 2010 (<https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf>). IPv6 technology, in accordance with the USGv6 Profile (NIST Special Publication (SP) 500-267 <http://www-x.antd.nist.gov/usgv6/index.html>), the Technical Infrastructure for USGv6 Adoption (<http://www.nist.gov/itl/antd/usgv6.cfm>), and the NIST SP 800 series applicable compliance (<http://csrc.nist.gov/publications/PubsSPs.html>) shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 users, and all internal infrastructure and applications shall communicate using native IPv6 operations. Information concerning IPv6 transition in addition to OMB/VA Memoranda can be found at <https://www.voa.va.gov/>.

**Previous Storage Procurements**: Where applicable, the Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) requirements and compliance standards established by FAR and NIST for IPv6 for Federal Government Agencies. IPv6 technology must be included in all infrastructure and application design and development efforts.

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 9 and Microsoft Office 2010.   Applications delivered to the VA and intended to be deployed to Windows XP or 7 workstation shall be delivered as a signed  .msi package and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA’s current desktop application deployment tool.   Signing of the software code shall be through a VA trusted code signing authority such as AT&T/Cybertrust or Symantec/VeriSign.  The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that has been configured using the Federal Desktop Core Configuration (FDCC) and United States Government Configuration Baseline (USGCB) specific to the particular client operating system being used.

The Contractor shall support VA efforts in accordance with the Project 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 OIT Project Managers and teams to meet their mission: delivering world-class IT products that meet business needs on time and within budget.

The Contractor shall utilize ProPath, the OIT-wide process management tool that assists in the execution of an IT project (including adherence to PMAS standards). It is a one-stop shop providing critical links to the formal approved processes, artifacts, and templates to assist project teams in facilitating their PMAS-compliant work. ProPath is used to build schedules to meet project requirements, regardless of the development methodology employed.

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

### POSITION/TASK RISK DESIGNATION LEVEL(S)

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

The position sensitivity and the level of background investigation commensurate with the required level of access for the tasks within the Performance Work Statement will be identified in individual orders.

The Tasks identified above and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the particular Contractor individual will be working. The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each Contractor individual based upon the tasks the Contractor individual will be working, in accordance with their submitted proposal.

###  CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

**Contractor Responsibilities:**

1. 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.
2. The Contractor shall bear the expense of obtaining background investigations.
3. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations. The roster shall contain the Contractor’s Full Name, Full Social Security Number, Date of Birth, Place of Birth, and individual background investigation level requirement (based upon Section 6.2 Tasks).
4. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
5. For a Low Risk designation the following forms are required to be completed: 1.OF-306 and 2. DVA Memorandum – Electronic Fingerprints. For Moderate or High Risk the following forms are required to be completed: 1. VA Form 0710 and 2. DVA Memorandum – Electronic Fingerprints. These should be submitted to the COR within 5 business days after award.
6. The Contractor personnel will receive an email notification from the Security and Investigation Center (SIC), through the Electronics Questionnaire for Investigations Processes (e-QIP) identifying the website link that includes detailed instructions regarding completion of the investigation documents (SF85, SF85P, or SF 86). The Contractor personnel shall submit all required information related to their background investigations utilizing the Office of Personnel Management’s (OPM) Electronic Questionnaire for Investigations Processing (e-QIP).
7. The Contractor is to certify and release the e-QIP document, print and sign the signature pages, and send them to the COR for electronic submission to the SIC. These should be submitted to the COR within 3 business days of receipt of the e-QIP notification email.
8. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
9. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or “Closed, No Issues” (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed “Contractor Rules of Behavior.” However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).
10. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
11. Failure to comply with the Contractor personnel security investigative requirements may result in termination of the contract for default.

## METHOD AND DISTRIBUTION OF DELIVERABLES

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

##  PERFORMANCE METRICS

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

|  |  |  |
| --- | --- | --- |
| ***Performance Objective*** | ***Performance Standard*** | ***Acceptable Performance Levels*** |
| 1. ***Technical Needs***
 | ***TBD*** | ***TBD*** |
| 1. ***Project Milestones and Schedule***
 | ***TBD*** | ***TBD*** |
| ***3. Project Staffing*** | ***TBD*** | ***TBD*** |
| ***4. Value Added*** | ***TBD*** | ***TBD*** |

The Government will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable manner. The Government reserves the right to alter or change the surveillance methods in 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.

## FACILITY/RESOURCE PROVISIONS

The Government will arrange a staging area for the delivery and inventory of equipment. All procedural guides, reference materials, and program documentation for the project and other Government applications will be provided on an as-needed basis.

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

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

VA will provide access to VA specific systems/network as required for execution of the task via remote access technology (e.g. Citrix Access Gateway (CAG), site-to-site VPN, or VA Remote Access Security Compliance Update Environment (RESCUE)). This remote access will provide access to 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 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.

## GOVERNMENT FURNISHED PROPERTY

### Government-Furnished Equipment (GFE)/Government-Furnished Information (GFI).

GFE determined necessary for performance under the contract will be provided. The COR will ensure that any GFE is properly accounted for in accordance with appropriate Federal, or organizational regulations. The Contractor will report any GFE not consumed in use during performance to the COR upon completion of the contract, and the COR will provide disposition instructions to the Contractor. VA EO Computing Services will provide space for any equipment the Contractor is required to install in VA EO’s facilities or other facilities as required. All equipment that the vendor proposes to install at the Government site will be outlined in the PWS.

### Configuration and Customization Rights and Non-Disclosure Agreement.

The Government shall have unlimited rights to all configuration and customization of software delivered including technical data and computer software, including the use of configuration and customized items after contract end. Contract will provide documentation of all configuration and customization done to software provided.

The Contractor shall have all employees working under this PWS to sign the Non-Disclosure of Non-Public Information and Conflict of Interest Form.

# ADDENDUM A

* 1. Cyber and Information Security Requirements for VA IT Services

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations.  The Contractor’s firewall and web server shall meet or exceed VA minimum requirements for security.  All VA data shall be protected behind an approved firewall.  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.

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

Each documented initiative under this contract incorporates VA Handbook 6500.6, “Contract Security,” March 12, 2010 by reference as though fully set forth therein. The VA Handbook 6500.6, “Contract Security” shall also be included in every related agreement, contract or order.  The VA Handbook 6500.6, Appendix C, is included in this document as Addendum B.

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS), and will be tracked therein. The TMS may be accessed at [https://www.tms.va.gov](https://www.tms.va.gov/). If you do not have a TMS profile, go to <https://www.tms.va.gov> and click on the “Create New User” link on the TMS to gain access.

Contractor employees shall complete a VA Systems Access Agreement if they are provided access privileges as an authorized user of the computer system of VA.

* 1. 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).  VA reserves the right to assess contract deliverables for EA compliance prior to acceptance.

**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>

* 1. Notice of the Federal Accessibility Law Affecting All Electronic and Information Technology Procurements  (Section 508)

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

* 1. 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. 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.  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.
	1. 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 toProtected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard (“Security Rule”).  Pursuant to the Privacy and Security Rules, the Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

1. The Contractor will have access to some privileged and confidential materials of VA.  These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA.  Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38.  Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA Contracting Officer will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information.  Any request for information relating to this contract presented to the Contractor shall be submitted to the VA Contracting Officer for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities.  Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract.  Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature.  If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract*,* the Contractor has a responsibility to ask the VA Contracting Officer.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information.  Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives.  The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
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.
17. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed.  In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.