



PERFORMANCE WORK STATEMENT (PWS)

**DEPARTMENT OF VETERANS AFFAIRS
Office of Information Technology
Enterprise Satellite Program Office**

Enterprise Satellite Communications

**Date: February 19, 2014
TAC-14-14274
PWS Version Number: 2.5.3**

Contents



.....	1
1.0 BACKGROUND.....	4
2.0 APPLICABLE DOCUMENTS	4
3.0 SCOPE OF WORK.....	5
4.0 PERFORMANCE DETAILS.....	6
4.1 PERFORMANCE PERIOD.....	6
4.2 PLACE OF PERFORMANCE.....	7
4.3 TRAVEL	7
5.0 SPECIFIC TASKS AND DELIVERABLES	7
5.1 PROJECT MANAGEMENT	7
5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN.....	7
5.1.2 REPORTING REQUIREMENTS	7
5.1.3 QUALITY CONTROL PLAN	8
5.1.4 KICK-OFF MEETING.....	9
5.1.5 MONTHLY CONFERENCE CALLS.....	9
5.1.6 TRANSITION PLANS	9
5.1.6.1 PHASE IN PLAN	9
5.1.6.2 PHASE OUT PLAN	10
5.2 ENTERPRISE SATCOM REQUIREMENTS	10
5.2.1 BANDWIDTH REQUIREMENT	11
5.3 ENTERPRISE SATCOM OPERATIONS.....	12
5.3.1 HUB OPERATIONS	12
5.3.2 VSAT (MOBILE) OPERATIONS.....	13
5.3.3 FIRST-RESPONDER SATCOM TERMINAL OPERATIONS (OPTIONAL TASK) 14	
5.3.4 EMERGENCY OPERATIONS SUPPORT (OPTIONAL TASK)	15
5.3.5 NATIONAL DRILLS & FIELD EXERCISE SUPPORT	15
5.3.5.1 NATIONAL DRILL SUPPORT	15
5.3.5.2 FIELD EXERCISE SUPPORT.....	16
5.4 ENTERPRISE SATCOM MAINTENANCE	16
5.4.1 HUB EQUIPMENT MAINTENANCE.....	16
5.4.2 VSAT EQUIPMENT MAINTENANCE.....	17
5.4.3 FIRST-RESPONDER EQUIPMENT MAINTENANCE (OPTIONAL TASK) 17	
5.4.4 ENTERPRISE SATCOM HARDWARE AND SOFTWARE.....	18
5.4.4.1 HUB EQUIPMENT	18
5.4.4.2 VSAT HARDWARE	18
5.4.4.3 SIP TELEPHONES REPLACEMENT.....	18
5.4.4.4 BLOCK UP CONVERTER (BUC) UPGRADE	19
5.4.4.5 VSAT TERMINALS (OPTIONAL TASK).....	19
5.4.4.6 RUGGEDIZED STORAGE CONTAINERS.....	19

Enterprise SatCom
TAC Number: TAC-14-14274

5.4.4.7	FIRST-RESPONDER SATELLITE UNITS (OPTIONAL TASK).....	20
5.4.5	ASSESSMENT AND ACCREDITATION SUPPORT	20
5.4.6	RETURN MERCHANDIZE AGREEMENT (RMA)	21
5.4.7	TRAINING REQUIREMENT	21
5.4.7.1	VSAT TRAINING	21
5.4.7.2	FIRST-RESPONDER TRAINING (OPTIONAL TASK)	22
5.4.8	HELP DESK SUPPORT	22
5.4.8.1	TIER 1 HELP DESK SUPPORT	22
5.4.8.2	TIER 2 AND TIER 3 HELP DESK SERVICES	24
5.5	OPTION PERIODS	25
5.5.1	OPTION PERIOD 1	25
5.5.2	OPTION PERIOD 2	25
5.5.3	OPTION PERIOD 3	25
5.5.4	OPTION PERIOD 4	26
6.0	GENERAL REQUIREMENTS	26
6.1	ENTERPRISE AND IT FRAMEWORK	26
6.2	POSITION/TASK RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS.....	27
6.2.1	POSITION/TASK RISK DESIGNATION LEVEL(S).....	27
6.2.2	CONTRACTOR PERSONNEL SECURITY REQUIREMENTS	29
6.3	METHOD AND DISTRIBUTION OF DELIVERABLES.....	30
6.4	PERFORMANCE METRICS.....	30
6.5	FACILITY/RESOURCE PROVISIONS	32
6.6	GOVERNMENT FURNISHED PROPERTY.....	33
ADDENDUM A	34
ADDENDUM B	39

1.0 BACKGROUND

Within the last decade, there have been significant hurricanes and tropical depressions, which have impacted the United States (U.S.): Charlie, Frances, Ivan, Jeanne, Katrina, Rita, Wilma, Ike, Gustav, Isaac and Sandy. Hurricane Katrina was responsible for significant devastation of the U.S. Gulf Coast. Hurricane Katrina caused the largest evacuation in the history of U.S. and cost the U.S. an estimated \$125 Billion. More recently, Super Storm Sandy caused an estimated \$20 Billion in damages. In almost all cases, because of these storms, service to our patients was disrupted due to the damaging effects. Also, recent attention has been given to a potential Pandemic flu outbreak.

In light of these facts and close evaluation of after action reports, Office of Information and Technology (OIT) identified a need to develop an Enterprise Satellite Communications (SatCom) infrastructure. The Enterprise SatCom Infrastructure consists of the VSAT Hubs, VSAT terminals, First-Responder terminals, operating on the same space segment (Ku-Band transponder bandwidth), and a terrestrial segment (teleport collocation services) to support VA continuity of operations for data, voice, and video communications. As OIT moves toward integrated regional and national data processing centers, it becomes even more critical that the Veteran Health Administration (VHA), Veterans Benefits Administration (VBA), and National Cemetery Administration (NCA) implement comprehensive contingent communications networks in support of consolidated operations.

2.0 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this PWS, the Contractor shall comply with the following:

1. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002"
2. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
3. FIPS Pub 201, "Personal Identity Verification of Federal Employees and Contractors," March 2006
4. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
5. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
6. Department of Veterans Affairs (VA) Directive 0710, "Personnel Suitability and Security Program," May 18, 2007
7. VA Directive 6102, "Internet/Intranet Services," July 15, 2008
8. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
9. OMB Circular A-130, "Management of Federal Information Resources," November 28, 2000
10. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008

11. 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
12. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
13. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, , 2012
14. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," September 20, 2012
15. VA Handbook 6500.1, "Electronic Media Sanitization," March 22, 2010
16. VA Handbook 6500.2, "Management of Data Breaches Involving Sensitive Personal Information (SPI)", January 6, 2012
17. VA Handbook 6500.3, "Certification and Accreditation of VA Information Systems," November 24, 2008
18. VA Handbook, 6500.5, "Incorporating Security and Privacy in System Development Lifecycle" March 22, 2010
19. VA Handbook 6500.6, "Contract Security," March 12, 2010
20. Project Management Accountability System (PMAS) portal (reference PWS References -Technical Library at <https://www.voa.va.gov/>)
21. 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.
22. Technical Reference Model (TRM) (reference at <https://www.voa.va.gov/>)
23. National Institute Standards and Technology (NIST) Special Publications
24. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008
25. OMB Memorandum, "Transition to IPv6", September 28, 2010
26. The Office of Management and Budget (OMB) Circular A-130, Appendix III; Security of Federal Information Resources.
27. National Institute of Standards and Technology (NIST) Special Publication, (SP) SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations.
28. National Institute of Standards and Technology (NIST) Special Publication, (SP) SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations.

3.0 SCOPE OF WORK

The Contractor shall operate and maintain the current Department of Veterans Affairs (VA) Enterprise SatCom infrastructure inclusive of supporting the satellite transponder operation, Radio Frequency (RF) chain components, teleport collocation services, Hub operation and Hub hardware / firmware components required to deliver private dedicated Enterprise SatCom services agency wide.

The Contractor is required to provide the following services:

- Program management support.
- Transition plans delineating the Phase-In and Phase-Out approaches.
- Operate and maintain satellite transponder and terrestrial operations.
- Emergency support during declared nationally declared disasters.
- Support hardware and software maintenance.
- Support on-site and remote training.
- Perform updates/replacements of hardware and software.
- Assessment & Accreditation (A&A) Documentation Support.
- Remote and on-site support.
- Helpdesk services.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance shall be one 12-month base period with four 12-month option periods.

Any work perform 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

4.2 PLACE OF PERFORMANCE

Tasks under this PWS shall be performed at Contractor facilities and at VA facilities as listed in Attachment 2.

4.3 TRAVEL

The Government anticipates travel under this effort to perform the tasks associated with the effort, as well as to attend program-related meetings or conferences through the period of performance. Include all estimated travel costs in your firm-fixed price line items. These costs will not be separately reimbursed by the Government.

VA anticipates a total of four (4) discretionary visits per year with duration of two (2) days each. The Contractor shall account for no more than two (2) personnel per trip. Historically this has been to a location within the 48 contiguous states. Travel to Enterprise SatCom locations requires prior approval from the Contracting Officer's Representative (COR) and/or Project Manager.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.1 PROJECT MANAGEMENT

5.1.1 CONTRACTOR 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 shall take the form of both a narrative and graphic format that displays the schedule, milestones, risks and resource support. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The initial baseline CPMP shall be concurred upon and updated monthly thereafter. The Contractor shall update and maintain the VA Project Manager (PM) approved CPMP throughout the period of performance.

Deliverable:

- A. Contractor Project Management Plan

5.1.2 REPORTING REQUIREMENTS

The Contractor shall provide the VA PM and COR with Monthly Progress Reports in electronic form in Microsoft Word and Microsoft Excel formats. Each Monthly Progress 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 month. Each Monthly Progress Report shall cover all work completed during the reporting period and work planned for the subsequent reporting period. The 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.

Deliverable:

- A. Monthly Progress Report

5.1.3 QUALITY CONTROL PLAN

The Contractor shall provide a Quality Control Plan that contains, at a minimum, the items listed below and shall be submitted to the Contracting Officer (CO) and COR for acceptance not later than the post award conference.

The Contractor shall provide a plan that includes:

1. A description of the Quality Control Plan to cover all services listed on the performance requirements metrics (see section 6.4). The description shall include specifics as to the areas to be inspected on both a scheduled and unscheduled basis, frequency of inspections, and the title and organizational placement of the inspectors. Additionally, control procedures for any government-provided keys or lock combinations must be included.
2. A description of the methods to be used for identifying and preventing defects in the quality of service performed.
3. A description of the records to be kept to document inspections and corrective or preventive actions taken.

The records of inspections shall be kept and made available to the CO and the COR, when requested, throughout the contract performance period and for the period after contract completion until final settlement of any claims under this contract.

Deliverable:

- A. Quality Control Plan

5.1.4 KICK-OFF MEETING

The Contractor shall schedule and provide proposed agenda for the Kick-Off Meeting to be held within ten (10) business days after contract award or as agreed upon between the Enterprise SatCom Program Office (ESPO), COR and the Contractor. In the Kick-Off Meeting the Contractor shall address post-award topics and provide a presentation to the ESPO team of the Contractor's plan and approach for meeting all PWS requirements. This shall include review of the CPMP and any outstanding comments from the COR/PM on the CPMP. The Kick-Off Meeting shall be a virtual meeting. At the conclusion of the Kick-Off Meeting the Contractor shall provide the VA PM and COR with the minutes.

5.1.5 MONTHLY CONFERENCE CALLS

The Contractor shall setup and coordinate on behalf of the VA PM monthly conference calls with representatives from the ESPO and the COR. The purpose of these monthly conference calls are to keep the ESPO team abreast of the current status of activities being performed on this contract, discuss pending issues (including actions being taken to resolve problems), and to provide project related recommendations. The Contractor shall document the relevant information resulting from these monthly conference calls in the Monthly Progress Report (refer to Section 5.1.2).

5.1.6 TRANSITION PLANS

5.1.6.1 PHASE IN PLAN

At the start of this contract, the Contractor is expected to participate in Phase-In discussions/meetings and work closely with ESPO staff and the current out-going VSAT contractor(s) to work out any residual transitioning topics to kick start this contract.

The Contractor shall provide a detailed transition plan that includes:

- Roster of key POCs with name, role, email address, and telephone numbers.
- Transition timeline with key milestones.
- Procedural manuals/guidelines.
- Templates used in day-to-day operations.
- Itemized list of additional equipment to be provided.
- Estimated downtime by site and unit.
- Process for transfer of on-hand inventory, if applicable.
- Transition checklist.
- Signed turnover agreements, if applicable.
- System design plan.
- Network architecture plan.

Deliverable:

- A. Phase-In Transition Plan

5.1.6.2 PHASE OUT PLAN

At the end of this contract, the Contractor is expected to participate in Phase-Out discussions/meetings and work closely with ESPO staff and the incoming contractor(s) to work out any residual transitioning topics require to help kick start the future contract.

The Contractor shall provide a detailed Phase-Out Transition Plan that includes:

- a. Roster of key POCs with name, role, email address and telephone numbers.
- b. Transition timeline with key milestones.
- c. Procedural manuals/guidelines.
- d. Templates used in day-to-day operations.
- e. Itemized list of additional equipment to be provided.
- f. Estimated downtime by site and unit.
- g. Process for transfer of on-hand inventory, if applicable.
- h. Transition checklist.
- i. Signed turnover agreements, if applicable.
- j. System design plan.
- k. Network architecture plan.

Deliverable:

- A. Phase-Out Transition Plan

5.2 ENTERPRISE SATCOM REQUIREMENTS

VA currently utilizes Enterprise SatCom infrastructure inclusive of the satellite transponder operation, Radio Frequency (RF) chain components, teleport collocation services, Hub operation and Hub hardware / firmware components required to deliver private dedicated Enterprise SatCom services agency-wide. VA Enterprise SatCom infrastructure consists of two ground stations referred to as Hubs. This consists of one fixed terminal and 137 mobile terminals, referred to as VSAT or mobile terminals. These are deployed throughout VA enterprise networks (refer to Attachment 2). The Contractor shall continue supporting the operations and deployment of all systems within the Enterprise SatCom infrastructure to provide mobile communications and continuity of operations across the VA to be used for supporting Veterans' medical care and emergency communications. The Enterprise SatCom infrastructure shall operate to provide contingent voice, video and data communications services via IP (Internet Protocol).

Enterprise SatCom
TAC Number: TAC-14-14274

Two Enterprise SatCom Hubs are deployed at South Jordan, Utah (UT) and Laurel, Maryland (MD). Addresses for the UT and MD Facilities are identified below:

Enterprise SatCom Hub Site #1
10288 S Jordon Gateway #K
South Jordan, UT 94095

Enterprise SatCom Hub Site #2
9898 Brewers Court
Laurel, MD 20723

As part of the VSAT Hubs operation, the Contractor shall maintain a primary and a secondary ground station (Hub) for redundancy purposes. As part of redundancy, these VSAT Hubs must be at least 500 miles apart geographically and reside in different time zones.

The Contractor shall update and maintain software, hardware, and licenses for the current Enterprise SatCom infrastructure by supporting existing and future circuit requirements. The Contractor shall maintain the dedicated private satellite network operating on 36 MHz of space segment on the transponder defined in Section 5.2. The outbound carriers shall operate at throughput of 17.5 Mbps. There will be up to thirteen inbound carriers that will operate between one to four Mbps. The total inbound throughput will be up to 15 Mbps. The inbound bandwidth shall be flexible and reconfigurable to accommodate larger carriers, dependent on need and link budget calculation.

The Contractor shall provide a 10 Mb terrestrial link to the Internet so the VSAT units can have direct Internet access. The Contractor shall provide a 100Mb Ethernet interface (copper RJ45) for accessing into a VA Network. The demarcation point of responsibility shall be the Network Security Operations Center (NSOC) managed firewall located at each Hub location (refer to Primary Hub Topology diagram). This is the boundary of the Enterprise SatCom Infrastructure and demarcation point for direct access to the VA Network.

5.2.1 BANDWIDTH REQUIREMENT

The Contractor shall provide, at a minimum, a dedicated, non-pre-emptible 36 MHz contiguous Ku Band transponder for use by the Enterprise SatCom infrastructure throughout the period of performance of this contract. The Ku Band satellite footprint shall cover Alaska, Hawaii, CONUS, Puerto Rico, and US Virgin Islands.

5.3 ENTERPRISE SATCOM OPERATIONS

5.3.1 HUB OPERATIONS

The Contractor shall provide Hub Operations at locations to be determined by the Awardee. Presently Hub Operations are being conducted and maintained by VETCORPS and currently located in South Jordan, Utah (UT) and Laurel, Maryland (MD). Upon award, the incoming Contractor shall coordinate with VETSCOPR the manner in which Hub Operations will transition. Awardee is not obligated to continue operations at the current locations. However, Awardee must be prepared to have independent operations by November 31, 2014.

The Contractor shall perform remote monitoring to ensure full operations of these hubs on 24x7x365 basis. The Contractor shall provide at least 99.99% uptime availability for HUB operations. The Contractor is expected to work on-site only in troubleshooting, emergency, or maintenance situations.

The Contractor shall support the following Hub operations services:

- a. Provide and manage bandwidth allocation for a minimum of 36 Mhz dedicated, non-pre-emptible transponder bandwidth, and ensure compatibility with existing Enterprise SatCom infrastructure and bandwidth services as currently provided by the Enterprise SatCom Program Office (ESPO).
- b. All satellite modem to modem connectivity shall be Advanced Encryption Standard (AES)-256 link encrypted.
- c. Assign and manage all multiple inbound and outbound carrier channels; fax and voice service hardware.
- d. Provide up-link frequency assignments to each remote terminal (VSAT and MicroSat).
- e. Provide down-link frequency assignments to each remote terminal (VSAT and MicroSat).
- f. Provide longitude and latitude assignments for each remote terminal (VSAT and MicroSat).
- g. Provision Hub Radio Frequency (RF) and networking resources for changes in remote site demographics and support special requests for Hub re-provisioning in the event of emergency operations requirements.
- h. Monitor and analyze the Enterprise SatCom network performance data to insure optimal operation of space segment components for Hub systems.
- i. Maintain Hub software / hardware and perform tasks related to the deployment, testing and field support of the Enterprise SatCom Hub communications delivery solutions.
- j. Ensure that Hub backup (failover) operations are tested and functional at all times. Function shall be tested quarterly.
- k. Provide technical assistance as required to resolve operational / expansion issues relating to the interface of Hub systems (both hardware and software).

Enterprise SatCom
TAC Number: TAC-14-14274

- I. Coordinate facility access with ESPO PM and COR when access to facility is required.
- m. Provide a Quarterly Hub Failover Test Report. The Quarterly Hub Failover Test Report shall capture all failover activities occurring in this period.
- n. Provide a Quarterly Change Report capture changes made to existing equipment or configuration (i.e. provisioning of circuits).
- o. Create the following Hub Operations documentations:
 - a. Enterprise SatCom Network Operations document In Accordance With (IAW) best commercial practices, and shall contain:
 - i. Antenna Controller configuration Router and switch configuration VoIP configuration.
 - ii. Dial Plan configuration.
 - iii. IP address planning.
 - iv. Unit and device naming convention Video conference configuration Printer setup.
 - b. Enterprise SatCom Implementation Diagrams document IAW best commercial practices.
 - c. Enterprise SatCom Network Security Overview document in compliance with NIST standards.

Deliverables:

- A. Quarterly Hub Failover Test Report
- B. Quarterly Change Report
- C. Enterprise SatCom Network Operations document
- D. Enterprise SatCom Implementation Diagrams document
- E. Enterprise SatCom Network Security Overview document

5.3.2 VSAT (MOBILE) OPERATIONS

The Enterprise SatCom's VSAT systems support a wide range of functions to include disaster response, emergency or temporary communications capabilities, direct patient care, national public health, and field conducted training. The VSAT inventory is identified in Attachment 2. The Contractor shall provide a least 99.9% of uptime availability for VSAT Operations.

The Contractor shall perform on-call operation support of these VSAT terminals. The Contractor shall provide the following VSAT on-call services:

- a. Provide remote support to VA users during routine testing and operational deployments to ensure the functionality of remote VSAT networking components.
- b. On a monthly basis provide VSAT operation service inputs to the Enterprise SatCom Utilization and Operations Reports to identify remote VSAT utilization / operations. Each monthly report shall address as a minimum the following:

Enterprise SatCom
TAC Number: TAC-14-14274

- i. Active inventory list by location.
 - ii. Bandwidth usage by each unit.
 - iii. Maximum bandwidth at the Hub in use over time (daily and monthly).
 - iv. Identify units that had zero usage during the reporting period.
-
- c. Maintain VSAT software / hardware and perform tasks related to the deployment, testing and field support of the VSAT systems.
 - d. Provide within 60 days of contract award an encrypted list of active passwords by location and provide updates as information changes.
 - e. Provide technical assistance as required to resolve operational issues relating to the interface of VSAT components (refer to Section 5.4.9 Help Desk Support).
 - f. Coordinate facility access with ESPO PM and COR when access to facility is required.

Deliverable:

- A. Monthly Enterprise SatCom Utilization and Operations Reports
- B. List of passwords (updated as required)

5.3.3 FIRST-RESPONDER SATCOM TERMINAL OPERATIONS (OPTIONAL TASK)

The Enterprise SatCom First-Responder satellite systems are used by VA's first responders. VA is migrating from the current L-Band Broadband Global Area Network (BGAN) man-portable terminals to the Ku-Band First Responder (man-portable) terminals (refer to Section 5.3.4.7 for specification).

When exercised, the Contractor shall perform the following First-Responder operation services:

- a. Provide remote support to VA First-Responder users during routine testing and operational deployments to ensure the functionality of remote man-portable networking components.
- b. Provide monthly inputs relating to the First-Responder operation service performed into the Enterprise SatCom Utilization and Operation Reports (refer to Section 5.3.2). Each monthly report shall address as a minimum the following:
 - i. Active inventory list by location
 - ii. Bandwidth usage by each unit
 - iii. Maximum bandwidth at the Hub in use over time (daily and monthly)
 - iv. Identify units that had zero usage during the reporting period
- c. Maintain Man-Portable software / hardware to latest versions.

- d. Provide within 60 days of contract award a list of active passwords by location and provide updates as information changes.
- e. Perform tasks related to the deployment, testing and field support of the First-Responder terminals.
- f. Provide technical assistance as required to resolve operational issues relating to the interface of First-Responder components.

Deliverable:

- A. List of passwords (updated as required)

5.3.4 EMERGENCY OPERATIONS SUPPORT (OPTIONAL TASK)

Upon a declared emergency, Enterprise SatCom VSAT terminals may be deployed to support the affected areas. When exercised, the Contractor shall provide the following emergency operation support:

- a. On-site engineering Subject Matter Expert (SME) support with:
 - i. Tools.
 - ii. Small repair kit.
- b. 24/7 hub provisioning support.
- c. Situational assessment.
- d. Bring the units involved to an operational status.
- e. Be prepared to be on-site for two days.
- f. Be on-site within 24 hours.
- g. Contact the ESPO for travel authority to enter into a disaster area.

5.3.5 NATIONAL DRILLS & FIELD EXERCISE SUPPORT

5.3.5.1 NATIONAL DRILL SUPPORT

VA conducts one annual National Drill that involves participation of Enterprise SatCom systems (VSAT Hubs, VSAT terminals and First-Responder terminals). The contractor shall provide two days of on-site support. Prior to the start of the National Drill, the Contractor shall participate in test planning meetings (if required).

The Contractor shall provide the following National Drill testing support:

- a. Acquaint National Drill Enterprise SatCom plans and procedures.
- b. Provide on-site engineering field support.
- c. Provide on-site knowledge transfers as needed.
- d. Provide a National Drill Enterprise SatCom After-Action Report detailing results of the National Drill event.

Deliverable:

- A. National Drill Enterprise SatCom After-Action Report

5.3.5.2 FIELD EXERCISE SUPPORT

The Contractor shall remotely provide quarterly field operations Enterprise SatCom testing support. Prior to the start of each test event, the Contractor shall participate in test planning meetings and provide the ESPO PM a detailed Field Operations Enterprise SatCom Testing Plan. The Field Operations Enterprise SatCom Testing Plan shall capture all Enterprise SatCom test milestones, procedures, and responsible parties.

The Contractor shall provide the following field operations Enterprise SatCom Testing support:

- a. Review the Enterprise SatCom plans and procedures.
- b. Coordinate test locations and times with the ESPO in advance, and have approval of the ESPO prior to execution.
- c. Document concise instructions and steps for the full operational testing of all remote Enterprise SatCom capabilities (voice, video and data).

The Contractor shall provide a Field Operations Enterprise SatCom After-Action Report detailing results of each field test.

Deliverables:

- A. Field Operations Enterprise SatCom Testing Plan
- B. Field Operations Enterprise SatCom After-Action Report

5.4 ENTERPRISE SATCOM MAINTENANCE

The Contractor shall perform on-going maintenance for all VSAT hardware, software, and licensing. Should a VSAT component not be repairable, it shall be replaced with a VSAT component of the same functionality. The replacement component must become the standard replacement item for the duration of the period of performance.

5.4.1 HUB EQUIPMENT MAINTENANCE

The Contractor shall perform on-going maintenance services (hardware, software and licenses) and necessary enhancements required to maintain all Hub Operations equipment at each Hub location. A full inventory of the Hub equipment can be found in Attachment 2.

The Contractor shall perform the following Hub equipment maintenance tasks:

- a. Perform routine and preventive maintenance on all equipment as prescribed by Original Equipment Manufacturer (OEM) recommended procedures and timeframes.
- b. Perform all emergency maintenance, when notified by VA PM or COR.
- c. Ensure the maintenance for both the primary and secondary Hubs are performed to the same level of maintenance quality as defined by OEM recommended procedures and timeframes.

Deliverable:

- A. Software Licenses

5.4.2 VSAT EQUIPMENT MAINTENANCE

The Contractor shall perform on-going maintenance services (hardware, software and licenses) and necessary replacements required to maintain all VSAT equipment. A full inventory of VSAT equipment can be found in Attachment 2.

The Contractor shall perform the following VSAT equipment maintenance tasks:

- a. Conduct routine and preventive maintenance on all existing equipment as prescribed by OEM recommended procedures and timeframes.
- b. Conduct routine and preventive maintenance of the newly acquired equipment shall start from time of installation through end of contract period of performance.
- c. Perform all emergency maintenance, when notified by VA PM.
- d. Conduct routine, preventive and emergency maintenance as prescribed by OEM recommended procedures and timeframes on newly acquired VSAT equipment under Section 5.4.4.5 thru 5.4.4.7.
- e. If equipment is deemed unsupportable, the Contractor shall inform and obtain the ESPO PM approval of the proposed change prior to performing the replacement.

Deliverable:

- A. Software Licenses

5.4.3 FIRST-RESPONDER EQUIPMENT MAINTENANCE (OPTIONAL TASK)

When exercised, the Contractor shall perform maintenance services (hardware, software and licenses) and necessary replacements required to maintain all First-Responder equipment, as defined in Section 5.4.4.7.

The Contractor shall perform the following First Responder equipment maintenance tasks:

- a. Conduct routine and preventive maintenance on all equipment, as prescribed by OEM recommended procedures and timeframes on man-portable equipment acquired from Section 5.4.4.7.
- b. Provide maintenance on the newly acquired equipment starting upon installation through the end of contract period of performance.
- c. Perform all emergency maintenance, when notify by VA PM.
- d. If equipment is deemed unsupportable, the Contractor shall inform and obtain ESPO PM approval for the proposed change prior to performing the replacement.

Deliverable:

- A. Software Licenses

5.4.4 ENTERPRISE SATCOM HARDWARE AND SOFTWARE

5.4.4.1 HUB EQUIPMENT

The Contractor shall use existing hardware, software, and licenses to continue to operate the current Enterprise SatCom Hubs.

5.4.4.2 VSAT HARDWARE

The Contractor shall use existing hardware, software, and licenses to continue to operate the current Enterprise SatCom VSAT terminals.

5.4.4.3 SIP TELEPHONES REPLACEMENT

The current inventory of wireless Session Initiation Protocol (SIP) telephones are unable to satisfy the requirement for AES-256 data encryption; it is necessary to replace all existing SIP phones in the Enterprise SatCom inventory. See Attachment 2 for an inventory of SIP phones. The Contractor shall replace existing wireless SIP telephones with the replacement SIP phones (See Attachment 1 for locations to ship).

Deliverable:

- A. 420 SIP Telephones

5.4.4.4 BLOCK UP CONVERTER (BUC) UPGRADE

The Enterprise SatCom VSAT user community has identified the need to upgrade the current Block Up Converter (BUC) to the existing VSAT terminals. The reason for the need to upgrade is due to the VSAT units being used for more bandwidth intensive applications and by more users than in the past. The current BUC standard is a four Watt Ku-Band BUC. VA requires these BUCs to be replaced with eight Watt BUCs. The replacement shall include all auxiliary components required to activate the eight Watt BUCs. VA currently has four eight-Watt BUCs in inventory. The Contractor shall deliver and install 134 eight-Watt BUCs during the initial performance period. The Contractor shall provide an installation schedule to complete the installation within a 12-month period. Refer to Attachment 1 for VSAT unit locations.

Deliverables:

- A. 134 Eight-Watt BUCs
- B. Installation schedule

5.4.4.5 VSAT TERMINALS (OPTIONAL TASK)

When exercised, the Contractor shall deliver up to eight VSAT Terminals available throughout the Period of Performance (PoP). Each new VSAT Terminal shall be fully compatible with existing deployed VSAT Terminals. The new VSAT Terminals shall have the same operating characteristics and set up procedures as the existing VSAT Terminals. This is required because VA has virtual VSAT operations teams and any operator within the VA may be expected to operate any VSAT terminals therefore mixed configuration and mixed operating procedures are not acceptable. Each new VSAT Terminal ordered shall include equipment, shipping, installation, activation, and user training. VA will provide a pre-configured or "VSAT ready" vehicle or location and the Contractor will not be responsible for facility or vehicle modifications. A new VSAT terminal shall consist of an auto-acquire dish, dish mounting hardware, controller, satellite modem, power supplies, router, switch, four SIP phones, wired analog phone, fax machine that is satellite communications compatible, copier/printer multifunction device, two wireless access points, and an IP-based video conferencing unit. See Attachment 2 for a complete inventory.

Deliverables:

- A. Up to eight VSAT Terminals

5.4.4.6 RUGGEDIZED STORAGE CONTAINERS

The Enterprise SatCom VSAT user community has identified a need for ruggedized storage containers. The Contractor shall provide 50 new ruggedized and padded plastic storage containers equipped with wheels, a handle, pressure relief valve and lock attachment points with following inside dimensions at a minimum 21"x21"X30".

The containers must meet Ingress Protection 67 rating standard. These storage containers shall be shipped to the Man Portable Units (MPU) locations designated in Attachment 1.

Deliverable:

- A. 50 Ruggedized Storage Containers

5.4.4.7 FIRST-RESPONDER SATELLITE UNITS (OPTIONAL TASK)

When exercised, the Contractor shall deliver up to ten Ku-Band First-Responder Terminals available throughout the PoP.

The Ku-Band man-portable terminals shall:

- a. Transmit at least one Mb uplink throughput and receiving four Mb of downlink throughput in support of user IP traffic.
- b. Weigh less than 50 pounds.
- c. Meet Mil Specification MIL-810F for test methods for Acceleration, Vibration, Sand, Dust, Rain, and Humidity.
- d. Encompass a setup time that does not exceed five minutes.
- e. Operate with alternate sources of power.
- f. Run on an included battery for 30 minutes.
- g. Support concurrent voice, video, and data using IPv4 and IPv6.
- h. Be compatible with and use the same bandwidth as the other 138 units.
- i. Have an automated mechanism for azimuth and elevation guidance.
- j. Have at least two RJ45 Ethernet interfaces.
- k. Be capable of operation on 12VDC or 120VAC power.
- l. Have a dish size no larger than 60cm.
- m. Include GPS, Compass, and level sensor.
- n. Allow for the storage and transport in a ruggedized storage containers.
- o. Be capable of Auto-acquire the satellite.
- p. Have Multiline phone capability.
- q. Provide Local encrypted WiFi for wireless users.
- r. Be airline checkable.

Deliverable:

- A. Up to ten Man-portable terminals

5.4.5 ASSESSMENT AND ACCREDITATION SUPPORT

The Contractor shall provide Authorization and Accreditation (A&A) documentation to support the Government's A&A activities, in accordance with the following guidelines:

- The Office of Management and Budget (OMB) Circular A-130, Appendix III; Security of Federal Information Resources.

- National Institute of Standards and Technology (NIST) Special Publication, (SP) SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations.
- National Institute of Standards and Technology (NIST) Special Publication, (SP) SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations.

The Contractor shall create and deliver A&A documents, as defined in the Accreditation Requirements Guide (see Attachment 3).

Deliverables:

- A. A&A Documentation

5.4.6 RETURN MERCHANDIZE AGREEMENT (RMA)

The Contractor shall provide a centralized Return Merchandise Agreement (RMA) program for the Enterprise SatCom Program. The Contractor shall support ESPO PM and field operations staff by utilizing hardware, software extended warranty maintenance, and shipping for the equipment described in Attachment 2.

5.4.7 TRAINING REQUIREMENT

5.4.7.1 VSAT TRAINING

The Contractor shall provide two consecutive days (eight hours per day) of on-site VSAT training and knowledge transfer at each of the 138 Enterprise SatCom unit locations. The Contractor will provide the ESPO PM with a proposed training schedule. As units are added to the Enterprise SatCom Network, they shall be included in the yearly training schedule. The training shall consist of:

- a. Instruction for up to 8 people.
- b. An overview of how satellite systems work.
- c. An overview of the system components.
- d. Hands-on instruction in the setup and use of each component.
- e. Hands-on instruction in basic trouble shooting techniques for the specific VSAT system type.
- f. One hard copy of the instructions in a three-ring binder.
- g. One soft copy of the instructions in said three-ring binder.
- h. Electronic soft copy provided to the COR via email.
- i. A training sign-off sheet for each of the trainees to sign.
- j. A paper inventory of the VSAT equipment at the time of the training.

Deliverables:

- A. Unit Specific Training Manuals
- B. Training schedule

5.4.7.2 FIRST-RESPONDER TRAINING (OPTIONAL TASK)

The Contractor shall provide two First Responder terminals for training. As units are added to the Enterprise SatCom Network they shall be added to the yearly training schedule. The training shall consist of:

- a. Instruction for up to eight people.
- b. An overview of how satellite systems work.
- c. An overview of the system components.
- d. Hands-on instruction in the setup and use of each component.
- e. Hands-on instruction in basic trouble shooting techniques for the specific VSAT system type.
- f. One hard copy of the instructions in a three-ring binder.
- g. One soft copy of the instructions in said three-ring binder.
- h. Electronic soft copy provided to the COR via email.
- i. A training sign off sheet.
- j. A paper inventory of the VSAT equipment at the time of the training.

Deliverables:

- A. Unit Specific Training Manuals
- B. Training schedule

5.4.8 HELP DESK SUPPORT

5.4.8.1 TIER 1 HELP DESK SUPPORT

The Contractor shall provide Tier 1 Help Desk support throughout the PoP. Tier 1 support is defined as the basic level of customer support. The Contractor help desk representative that mans the phone is a generalist with a broader understanding of the product, but might not understand the inner workings of the system. The Contractor help desk representative shall identify and log the caller's issue, understand the problem, and provide problem resolution.

The requirement of the Tier 1 Help desk support services is as follows:

1. Shall provide helpdesk call number(s).
2. Shall document a Monthly Help Desk Report to the ESPO PM, and serve as the first tier of support for any required equipment replacements due to operational failure and any software upgrades that become required.

Enterprise SatCom
TAC Number: TAC-14-14274

3. Shall maintain a Contractor Trouble Ticket system, and records of all trouble ticket resolutions. All received trouble tickets shall be resolved within 48 hours unless specific guidance is provided by the COR stating otherwise.
4. Shall provide e-mail and telephone help desk customer support from 7:00 AM to 9:00 PM Eastern Time (ET) Monday through Friday.
5. Shall respond to 24x7 emergency telephone requests within two hours of initial call;
6. Shall respond to at least 80 percent of initial e-mail requests made during regular business hours within one hour and the remainder within three hours.
7. Shall respond to email requests sent after hours on the next business day.
8. Shall maintain a Contractor Trouble Ticket system, and records of all trouble ticket resolutions. All received trouble tickets shall be resolved within 48 hours unless specific guidance is provided by the COR stating otherwise.
9. Shall Provide e-mail and telephone help desk customer support from 7:00 AM to 9:00 PM ET Monday through Friday.
10. Shall respond to 24x7 emergency telephone requests within two hours of initial call;
11. Shall respond to at least 80 percent of initial e-mail requests made during regular business hours within one hour and the remainder within three hours.
12. Shall respond to email requests sent after hours on the next business day.
13. Shall provide a response/acknowledgement within one business day for all customer inquiries.
14. Shall respond to requests for password resets and other account issues utilizing the same performance standards for all help desk requests.
15. Shall maintain a Help Desk application to track trouble tickets and assist with troubleshooting.
16. Shall host monthly Enterprise SatCom Support Team calls to assist with workflow and issue resolution.
17. Shall provide summary help desk information in the Monthly help desk Report (see Section 5.1.2) for all Tier 1, 2 and 3 help desk activities, to include:
 - A. Number of response calls (trouble tickets processed) for each month
 - B. Type of Tier support of each call
 - C. Unit and Location of the caller
 - D. Reason for call and resolution
 - E. Response time and resolution activities
 - F. Problems encountered in restoring units to operational readiness
 - G. Timeliness of Response Calls
18. Shall interface with Enterprise SatCom operators.
19. Shall support national independent field testing of Enterprise SatCom units by annotating work orders placed during the tests.
20. Shall interface with field OI&T help desks.
21. Shall support local OI&T staffs with Enterprise SatCom configurations and other Enterprise SatCom technical issues.
22. Shall report all application issues to the ESPO within 24 hours.
23. Shall maintain current inventory of all Enterprise SatCom Equipment in the automated inventory system.

Deliverable:

A. Monthly Help Desk Report

5.4.8.2 TIER 2 AND TIER 3 HELP DESK SERVICES

The Contractor shall provide a Tier 2 / 3 help desk trouble ticket system with monthly help desk reports sent to the ESPO PM, and serve as the liaison for required equipment replacements due to operational failure and software upgrades that become required.

The requirement of the Tier 2 / 3 Help desk support services is as follows:

1. Shall be accessible during normal operations from 7:00am to 9pm ET via email and telephone support.
2. Shall have available 24x7 telephone support for emergency calls.
3. Shall provide e-mail and telephone help desk customer support from 7:00 AM to 9:00 PM ET Monday through Friday.
4. Shall respond to 24x7 emergency telephone requests within two hours of initial call.
5. Shall respond to at least 80 percent of initial e-mail requests made during regular business hours within one hour and the remainder within three hours.
6. Shall respond to email requests sent after hours on the next business day.
7. Shall provide a response/acknowledgement within one business days for all customer inquiries.
8. Shall respond to requests for password resets and other account issues utilizing the same performance standards for all help desk requests.
9. Shall maintain a Help Desk application to track trouble tickets and assist with troubleshooting.
10. Shall host weekly Enterprise SatCom Support Team calls to discuss on workflow and issue resolution.
11. Shall provide summary information in the Monthly Testing Report to Tier 3 SME of all help desk activities, to include the number of trouble tickets processed in a month, response time and resolution activities.
12. Shall interface with Enterprise SatCom operators.
13. Shall support national independent field testing of Enterprise SatCom units by annotating work orders placed during the tests.
14. Shall interface with field OIT Help Desks.
15. Shall support local OIT staffs with Enterprise SatCom configurations and other Enterprise SatCom technical issues.
16. Shall report all application issues to the ESPO PM within twenty-four hours.
17. Shall performs on-site installation of equipment, and report equipment inventory for remote (downlink) Enterprise SatCom locations and networking systems equipment at the Hub locations.
18. Shall perform on-site installation, inventory configuration and training for equipment changes or upgrades of Enterprise SatCom units supplied by the Government.

19. Shall establish an Enterprise SatCom equipment inventory database to insure accurate accountability for all Enterprise SatCom components; the inventory database must have a field for recording instances of broken equipment. Broken equipment must be reported in the Monthly Testing Reports.
20. Shall maintain current inventory of all Enterprise SatCom Equipment in the automated inventory system and report activities into Quarterly Enterprise SatCom Inventory Reports.

Deliverable:

- A. Quarterly Enterprise SatCom Inventory Reports

5.5 OPTION PERIODS

5.5.1 OPTION PERIOD 1

If the Option Period is exercised by VA, the Contractor shall perform all the tasks identified in Sections 5.1 thru 5.4.8.2 with the exception of Sections 5.1.3 (Quality Control Plan), 5.1.4 (Kick-Off Meeting), 5.1.6.1 (Phase-In Plan), 5.4.4.3 (SIP Telephone Replacement), 5.4.4.4 (Block-Up Converter (BUC) Upgrade), 5.4.4.6 (Ruggedized Storage Containers), and 5.4.5 (Assessment and Accreditation Support) throughout the duration of Option Period 1.

5.5.2 OPTION PERIOD 2

If the Option Period is exercised by VA, the Contractor shall perform all the tasks identified in Sections 5.1 thru 5.4.8.2 with the exception of Sections 5.1.3 (Quality Control Plan), 5.1.4 (Kick-Off Meeting), 5.1.6.1 (Phase-In Plan), 5.4.4.3 (SIP Telephone Replacement), 5.4.4.4 (Block-Up Converter (BUC) Upgrade), 5.4.4.6 (Ruggedized Storage Containers), and 5.4.5 (Assessment and Accreditation Support) throughout the duration of Option Period 2.

5.5.3 OPTION PERIOD 3

If the Option Period is exercised by VA, the Contractor shall perform all the tasks identified in Sections 5.1 thru 5.4.8.2 with the exception of Sections 5.1.3 (Quality Control Plan), 5.1.4 (Kick-Off Meeting), 5.1.6.1 (Phase-In Plan), 5.4.4.3 (SIP Telephone Replacement), 5.4.4.4 (Block-Up Converter (BUC) Upgrade), 5.4.4.6 (Ruggedized Storage Containers), and 5.4.5 (Assessment and Accreditation Support) throughout the duration of Option Period 3.

5.5.4 OPTION PERIOD 4

If the Option Period is exercised by VA, the Contractor shall perform all the tasks identified in Sections 5.1 thru 5.4.8.2 with the exception of Sections 5.1.3 (Quality Control Plan), 5.1.4 (Kick-Off Meeting), 5.1.6.1 (Phase-In Plan), 5.4.4.3 (SIP Telephone Replacement), 5.4.4.4 (Block-Up Converter (BUC) Upgrade), 5.4.4.6 (Ruggedized Storage Containers), and 5.4.5 (Assessment and Accreditation Support) throughout the duration of Option Period 4.

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

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.

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/>.

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. However, the migration from Windows XP to Windows 7 is not yet complete within all of VA. As a result, compatibility with and support on Windows XP, Internet Explorer 7 and Microsoft Office 2007 are also required until April 2014 when Microsoft's extended support for Windows XP ends. 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 Verizon/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.

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

6.2.1 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.

Enterprise SatCom
TAC Number: TAC-14-14274

Position Sensitivity	Background Investigation (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Security Suitability Program," Appendix A)
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 following tasks within the Performance Work Statement are:

	Position Sensitivity and Background Investigation Requirements		
<u>Task Number</u>	<u>Low/NACI</u>	<u>Moderate/MBI</u>	<u>High/BI</u>
5.1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

- a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
- b. The Contractor shall bear the expense of obtaining background investigations.
- c. 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).
- d. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
- e. 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.
- f. The Contractor personnel will receive an email notification from the Security and Investigation Center (SIC), through the Electronics Questionnaire for Investigations Processes (e-QIP) identifying the website link that includes detailed instructions regarding completion of the investigation documents (SF85, SF85P, or SF 86). The Contractor personnel shall submit all required information related to their background investigations utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP).
- g. The Contractor is to certify and release the e-QIP document, print and sign the signature pages, and send them to the COR for electronic submission to the SIC. These should be submitted to the COR within 3 business days of receipt of the e-QIP notification email.
- h. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
- i. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or "Closed, No Issues" (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must

be maintained in the database of the Office of Personnel Management (OPM).

- j. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
- k. Failure to comply with the Contractor personnel security investigative requirements may result in termination of the contract for default.

6.3 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).

6.4 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
5.1.1 Contractor Project Management Plan (CPMP).	Ten (10) business days after contract award or as agreed upon between the VA COR and contractor. Meeting minutes shall be distributed for review and comment three (3) business days after the meeting. Updated, final version five (5) business days after meeting.	100% Compliance
5.1.2 Reporting Requirements	Monthly Progress Report to include detailed instructions/explanation for each required element to insure data is accurate and consistent in electronic form in Microsoft Word and Excel formats.	2 or fewer instances of deviations from the approved processes without prior approval within a 12 month contract period.
5.1.3 Quality Control Plan	Detailed plan of quality assurance procedures used to measure, track and Report contract performance to include list of services, description of methods and description of records.	2 or fewer instances of deviations from the approved processes without prior approval within a 12 month contract

Enterprise SatCom
TAC Number: TAC-14-14274

Performance Objective	Performance Standard	Acceptable Performance Levels
5.1.4 Kick-Off Meeting	The contractor shall schedule the Kick-Off Meeting to be held within ten (10) business days after contract award or as agreed upon between the VA COR and contractor. Meeting minutes shall be distributed for review and comment one (1) business day after the meeting. Updated, final version three (3) business days after meeting.	100% Compliance
5.1.5 Monthly Conference Calls	Keep the ESPO team abreast of the current status of activities being performed on this contract, discuss pending issues (including actions being taken to resolve problems), and to provide project related recommendations.	2 or fewer instances of deviations from the approved processes without prior approval within a 12 month contract period.
5.1.6.1 Transition Phase In Plan	Participate in Phase-In discussions/meetings and work closely with ESPO staff and the current outgoing VSAT contractor(s) to work out any residual transitioning topics require to help kick start this contract.	Satisfactory or higher
5.1.6.2 Transition Phase Out Plan	At the end of this contract, the Contractor is expected to participate in Phase-Out discussions/meetings and work closely with ESPO staff and the ingoing contractor(s) to work out any residual transitioning topics require to help kick start the future contract.	100% Compliance
5.1.6.1 Transition Phase In Plan	Monthly Progress Report detailing Current activities, discuss pending issues (including actions being taken to resolve problems) and provide related recommendations.	100% Compliance
5.2 Enterprise SATCOMM Requirements	All activities shall be completed within the agreed to timeframe.	2 or fewer instances of deviations from the approved processes without prior approval within a 12 month contract period.
5.2.1 Bandwidth Requirement	All activities shall be completed within the agreed to timeframe.	2 or fewer instances of deviations from the approved processes without prior approval within a 12 month contract period.
5.3 Enterprise SATCOMM Operations	All activities shall be completed within the agreed to timeframe.	2 or less instances where an agreed upon timeframe for activities completion is not met during a 12 month contract period.

Performance Objective	Performance Standard	Acceptable Performance Levels
5.3.1 HUB Operations	99.99% Availability	2 or less instances where an agreed upon timeframe for activities completion is not met during a 12 month contract period.
5.3.2 VSAT (Mobile) Operations	99.9% Availability	2 or less instances where an agreed upon timeframe for activities completion is not met during a 12 month contract period.

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.

6.5 FACILITY/RESOURCE PROVISIONS

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 and ADDENDUM B.

6.6 GOVERNMENT FURNISHED PROPERTY

All Government Furnished Equipment (GFE) in Attachment 2 is in working order and under maintenance at this time. All GFE furnished to the Contractor will remain the property of VA and can only be disposed of as per Government regulation. All vehicles used with the Enterprise SatCom infrastructure are GFE. On expiration of the contract, the Contractor shall return to the PM all VA-owned equipment in the contractor's possession.

ADDENDUM A

A1.0 Cyber and Information Security Requirements for VA IT Services

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations. The Contractor's firewall and web server shall meet or exceed VA minimum requirements for security. All VA data shall be protected behind an approved firewall. 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>. If you do not have a TMS profile, go to <https://www.tms.va.gov> and click on the "Create New User" link on the TMS to gain access.

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

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at <http://www.ea.oit.va.gov/index.asp> in force at the time of issuance of this contract, including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP). VA reserves the right to assess contract deliverables for EA compliance prior to acceptance.

A2.1. VA Internet and Intranet Standards:

The Contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the Contractor's work includes managing, maintaining, establishing and presenting information on VA's Internet/Intranet Service Sites. This pertains, but is not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

A3.0 Notice of the Federal Accessibility Law Affecting All Electronic and Information Technology Procurements (Section 508)

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

- ☒ § 1194.21 Software applications and operating systems
- ☒ § 1194.22 Web-based intranet and internet information and applications
- ☒ § 1194.23 Telecommunications products
- ☒ § 1194.24 Video and multimedia products
- ☒ § 1194.25 Self contained, closed products
- ☒ § 1194.26 Desktop and portable computers

- ☒ § 1194.31 Functional Performance Criteria
☒ § 1194.41 Information, Documentation, and Support

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

A4.0 Physical Security & Safety Requirements:

The Contractor and their personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property. Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. 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.

A5.0 Confidentiality and Non-Disclosure

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

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

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use

only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.

2. The VA Contracting Officer will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA Contracting Officer for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA Contracting Officer.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
 - a. The use of "thumb drives" or any other medium for transport of information is expressly prohibited.
 - b. Controlled access to system and security software and documentation.
 - c. Recording, monitoring, and control of passwords and privileges.
 - d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.

Enterprise SatCom
TAC Number: TAC-14-14274

- e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
 - f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
 - g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
 - h. Contractor does not require access to classified data.
8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
9. 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.

ADDENDUM B

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

B1. GENERAL

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

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

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

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

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

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

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

B3. VA INFORMATION CUSTODIAL LANGUAGE

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

2. VA information should not be co-mingled, if possible, with any other data on the Contractor/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA information is returned to VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

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

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

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

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

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

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

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

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

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

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or a Memorandum of Understanding-

Interconnection Service Agreement (MOU-ISA) for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

N/A

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

N/A

B6. SECURITY INCIDENT INVESTIGATION

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

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

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

d. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The Contractor, its employees, and its Subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/Subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third

party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

B7. LIQUIDATED DAMAGES FOR DATA BREACH

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

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

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

- 1) Nature of the event (loss, theft, unauthorized access);
- 2) Description of the event, including:
 - a) date of occurrence;
 - b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
- 3) Number of individuals affected or potentially affected;
- 4) Names of individuals or groups affected or potentially affected;
- 5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
- 6) Amount of time the data has been out of VA control;
- 7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
- 8) Known misuses of data containing sensitive personal information, if any;
- 9) Assessment of the potential harm to the affected individuals;

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

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

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

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

B8. SECURITY CONTROLS COMPLIANCE TESTING

N/A

B9. TRAINING

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

- 1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems;
- 2) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* training and annually complete required security training;
- 3) Successfully complete *Privacy and HIPAA Training* if Contractor will have access to PHI;
- 4) Successfully complete the appropriate VA privacy training and annually complete required privacy training; and

Enterprise SatCom
TAC Number: TAC-14-14274

5) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access

- b. The Contractor shall provide to the contracting officer and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.
- c. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.