



PERFORMANCE WORK STATEMENT (PWS) FOR THE

**Austin Information Technology Center (AITC)
Emergency Diesel Generators System (EDGS) Repairs and Parts Contract**

Date: March 9, 2016

Version 1.7

**Department of Veteran Affairs
Office of Information & Technology
Austin Information Technology Center (AITC)**

AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826

Contents

1.0	BACKGROUND AND SCOPE.....	4
1.1	BACKGROUND	4
1.2	SCOPE	4
2.0	APPLICABLE DOCUMENTS	4
3.0	GENERAL REQUIREMENTS	6
3.1	CONTRACT TYPE.....	7
3.2	PERIOD OF PERFORMANCE.....	7
3.3	PLACE OF PERFORMANCE.....	7
3.4	TRAVEL OR SPECIAL REQUIREMENTS.....	7
3.5	MATERIALS AND EQUIPMENT	8
3.5.1	GOVERNMENT-FURNISHED.....	8
3.5.2	CONTRACTOR-ACQUIRED	8
3.5.3	NON-DEVELOPMENTAL ITEMS AND COMMERCIAL PROCESSES	8
3.5.4	CONNECTIVITY	8
3.5.5	WARRANTY	8
3.5.6	MARKING, HANDLING, STORAGE, PRESERVATION, PACKAGING, & SHIPPING	8
3.6	SAFETY AND ENVIRONMENTAL.....	8
3.7	ENTERPRISE AND IT FRAMEWORK.....	9
3.8	METHOD AND DISTRIBUTION OF DELIVERABLES	9
3.9	TRANSITION AND ORIENTATION SUPPORT	9
4.0	FUNCTIONAL AREAS	9
4.1	PROGRAM MANAGEMENT SUPPORT.....	9
4.2	GENERATOR MAINTENANCE EQUIPMENT	9
4.3	GENERATOR WARRANTY SUPPORT.....	10
4.4	MASTER CONTROL STATIONS (MCS) SUPPORT	11
4.5	GENERATOR MAINTENANCE	11
4.5.1	PREVENTIVE MAINTENANCE	12
4.5.2	ODD-YEAR MAINTENANCE.....	12
4.6	GENERATOR TESTING	12
4.6.1	WEEKLY GENERATOR TESTING	13
4.6.2	EARLY-YEAR and MID-YEAR LOAD TEST.....	16
4.6.3	ANNUAL EARLY-YEAR LOAD TEST	17
4.6.3.1	FLUID LAB ANALYSIS.....	18
4.6.3.2	INFRARED SCANNING	18
4.6.4	ANNUAL MID-YEAR LOAD TEST.....	18
4.7	EMERGENCY REPAIRS/NON-EMERGENCY REPAIRS (T&M).....	19
5.0	DELIVERABLES	20
5.1	PRODUCTS.....	20
5.2	DATA	20
6.0	SECURITY AND PRIVACY	21
6.1	INFORMATION SECURITY AND PRIVACY SECURITY REQUIREMENTS...	21
6.2	POSITION/TASK RISK DESIGNATION LEVEL(S).....	21

**AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826**

6.3	FACILITY/RESOURCE PROVISIONS	22
6.4	BADGES	22
7.0	REPORTING AND MEETING REQUIREMENTS	22
7.1	REPORTING REQUIREMENTS	22
7.2	MEETINGS AND REVIEWS	22
7.2.1	PROJECT OFFICE INITIAL PROGRAM REVIEW (IPR)	22
7.2.2	POST-AWARD CONFERENCES	23
ADDENDUM B- VA INFORMATION AND INFORMATION SYSTEM SECURITY / PRIVACY LANGUAGE		24

AITC EDGS REPAIRS & PARTS CONTRACT TAC-16-23826

1.0 BACKGROUND AND SCOPE

1.1 BACKGROUND

The mission of the Department of Veterans Affairs (VA), Office of Information & Technology (OI&T), Austin Information Technology Center (AITC) is to provide benefits and services to Veterans of the United States. In meeting these goals, OI&T strives to provide high quality, effective, and efficient Information Technology (IT) services to those responsible for providing care to the Veterans at the point-of-care as well as throughout all the points of the Veterans' health care in an effective, timely and compassionate manner. VA depends on Information Management/Information Technology (IM/IT) systems to meet mission goals.

The AITC processes data that is considered a lifeline to Veterans and constant availability of that data is crucial. The AITC facilities department is responsible for ensuring the data center will not experience any power loss or electrical outage under any circumstance, 24 hours a day and seven days a week (24/7). In support of these efforts, the Emergency Diesel Generator System (EDGS), located at the AITC, consists of six (6) Cummins brand name generators and associated equipment operated through the Cummins Master Control Station (MCS). Contractor services are required to remotely monitor the system 24/7 and provide maintenance, repair and on-call services for the generator equipment and associated wiring.

1.2 SCOPE

The Contractor shall provide VA generator maintenance to include project management, weekly testing, load testing, inspection, emergency and non-emergency repairs, associated reports, and the procurement and installation of required parts.

This Performance Work Statement (PWS) provides general requirements. Specific requirements shall be defined in individual Task Orders (TOs). Functional area requirements are described in PWS Section 4.0 and are not mutually exclusive for TO requirements. Requirements may fall within one specific functional area but in many cases, the requirements will encompass and apply across multiple functional areas to provide the total life cycle solution.

2.0 APPLICABLE DOCUMENTS

The Contractor shall comply with the documents listed below. Additional documents may be listed in individual TOs.

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 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013
4. 10 U.S.C. § 2224, "Defense Information Assurance Program"
5. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"

AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826

6. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
7. VA Directive 0710, "Personnel Suitability and Security Program," June 4, 2010, <http://www.va.gov/vapubs/>
8. VA Handbook 0710, Personnel Suitability and Security Program, September 10, 2004, <http://www.va.gov/vapubs>
9. VA Directive and Handbook 6102, "Internet/Intranet Services," July 15, 2008
10. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
11. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," November 28, 2000
12. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
13. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
14. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, 2012
15. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," March 10, 2015
16. VA Handbook 6500.1, "Electronic Media Sanitization," November 03, 2008
17. VA Handbook 6500.3, "Assessment, Authorization, And Continuous Monitoring Of VA Information Systems," February 3, 2014
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. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008
21. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, February 17, 2011
22. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 20, 2014 OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
23. OMB Memorandum 05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005
24. OMB memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011 OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
25. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
26. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
27. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
28. Draft NIST Special Publication 800-157, Guidelines for Derived PIV Credentials, March 2014

**AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826**

29. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
30. VA Memorandum, VAIQ #7100147, Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12), April 29, 2011 (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>)
31. VA Memorandum, VAIQ # 7011145, VA Identity Management Policy, June 28, 2010 (reference Enterprise Architecture Section, PIV/IAM (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>))
32. IAM Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, PIV/IAM (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>))
33. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, Department of Homeland Security, October 1, 2013, https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf
34. VA Memorandum, VAIQ #7497987, Compliance – Electronic Product Environmental Assessment Tool (EPEAT) – IT Electronic Equipment, August 11, 2014 (reference Document Libraries, EPEAT/Green Purchasing Section, <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=552>)
35. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
36. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
37. Executive Order 13514, “Federal Leadership in Environmental, Energy, and Economic Performance,” October 5, 2009
38. Executive Order 13423, “Strengthening Federal Environmental, Energy, and Transportation Management,” January 24, 2007
39. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
40. VA Directive 0058, “VA Green Purchasing Program”, July 19, 2013
41. VA Handbook 0058, “VA Green Purchasing Program”, July 19, 2013
42. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
43. NFPA (National Fire Protection Association) 110, “Standard for Emergency and Standby Power Systems”, January 1, 2013
44. Cummins Power Generation Warranty Statements, Generator Sets, and Commercial Standby Extended Warranty Statements

3.0 GENERAL REQUIREMENTS

The Contractor shall provide and/or acquire the services, hardware, and software required by each individual TO pursuant to the general requirements specified below.

**AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826**

3.1 CONTRACT TYPE

This is an Indefinite Delivery/Indefinite Quantity (IDIQ) single award contract. Individual TOs shall be issued on a performance-based Time-and-Materials (T&M) and/or Firm-Fixed-Price (FFP) basis.

3.2 PERIOD OF PERFORMANCE

The period of performance for the basic contract shall be 34-months from the effective date of award.

Work at a Government site shall not take place on Federal holidays or weekends (but may require off-hour work due to network loading or other disruptions that could occur) unless directed by the Contracting Officer (CO). The Contractor may also be required to support 24/7 operations 365 days per year as identified in individual TOs.

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

3.3 PLACE OF PERFORMANCE

The equipment under maintenance is located in the VA AITC facilities at 1615 Woodward Street, Austin, TX 78772. The place of performance shall be identified in the individual TOs.

3.4 TRAVEL OR SPECIAL REQUIREMENTS

No travel is authorized for this effort.

**AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826**

3.5 MATERIALS AND EQUIPMENT

3.5.1 GOVERNMENT-FURNISHED

Not Applicable

3.5.2 CONTRACTOR-ACQUIRED

The Contractor shall acquire and/or provide any hardware and/or software required to accomplish each TO that is not provided as GFP. Software integrity shall be maintained by the Contractor within the licensing agreement of the producer until such software is delivered to the Government, or otherwise disposed of in accordance with Government direction. Reference PWS Section 6.0 for detailed security requirements.

3.5.3 NON-DEVELOPMENTAL ITEMS AND COMMERCIAL PROCESSES

Non-Developmental Items (NDI), Commercially-Available-Off-The-Shelf (COTS) and Government-Off-The-Shelf (GOTS) products shall be used to the maximum extent. The Contractor shall apply commercially available and industry best processes, standards and technologies to the maximum extent.

3.5.4 CONNECTIVITY

VA will provide the Contractor use of Virtual Private Network (VPN) or Citrix Access Gateway (CAG) as appropriate. The Contractor will bear the cost to provide connectivity to the VA through VPN, and VA will provide the required account access accordingly. Other connectivity to VA systems may be authorized as appropriate in the individual TOs.

3.5.5 WARRANTY

Items acquired under this contract may require warranty protection. Commercial warranties shall be transferred to the Government. The type of warranty and extent of coverage shall be determined on an individual TO basis.

3.5.6 MARKING, HANDLING, STORAGE, PRESERVATION, PACKAGING, & SHIPPING

The Contractor shall establish/maintain procedures for handling, storage, preservation, packaging, and shipping to protect the quality of products and prevent damage, loss, deterioration, degradation or substitution of products.

3.6 SAFETY AND ENVIRONMENTAL

Safety and environmental procedures shall be identified in individual TO requirements.

The Contractor shall comply with the Office of Federal Procurement Policy Green Acquisition initiatives as identified in individual TOs in accordance with the policies referenced at http://www.whitehouse.gov/omb/procurement_index_green.

**AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826**

3.7 ENTERPRISE AND IT FRAMEWORK

Not Applicable

3.8 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).

3.9 TRANSITION AND ORIENTATION SUPPORT

The Contractor shall perform transition and orientation services (e.g. develop Phase-In/Phase-Out Transition Plan) to insure continuity of services as specified in the individual TO. Transition and orientation support may include transitioning to Government or Contractor personnel.

4.0 FUNCTIONAL AREAS

Individual TOs may encompass more than one functional area listed below. Functional area requirements are not mutually exclusive and may apply across multiple functional areas.

4.1 PROGRAM MANAGEMENT SUPPORT

The Contractor shall provide project and/or program management support to accomplish the administrative, managerial, logistical, integration and financial aspects specified in individual TOs. The Contractor shall provide and maintain a Contractor Personnel Emergency Contact List to include contact phone numbers. This list may be periodically checked for response. In addition, the Contractor shall provide the stationary diesel generator repair technician certificates for personnel performing the maintenance and repair tasks below.

Deliverable:

- A. Contractor Personnel Emergency Contact List
- B. Technician Certificates

4.2 GENERATOR MAINTENANCE EQUIPMENT

The Contractor shall provide maintenance solutions for the following generator equipment and associated wiring under this IDIQ:

- A. One Cummins (Generator #1) 750kW diesel generator set Model KTA38GS1 (with on-board Power Command digital paralleling system) with lead-acid starting batteries and charger, and other attached components including dampers.

AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826

- B. Two Cummins (Generators #2 and #3) 900kW diesel generator set Model 900DFJC (with on-board Power Command digital paralleling system) with lead-acid starting batteries and charger, and other attached components including dampers.
- C. One Cummins (Generator #4) 1000kW diesel generator set Model 1000DQFAD (with on-board Power Command digital paralleling system) with lead-acid starting batteries, battery charger, generator enclosure and other attached components including dampers.
- D. Three 400 amp Onan Model BT400 automatic transfer switches
- E. One 1000 amp Onan Model BT1000 automatic transfer
- F. One 3000 amp Onan BI automatic transfer switch
- G. Two emergency generator switchboards (EDAB and PSBD)
- H. One 3000 amp emergency power system disconnects
- I. One 3000 amp utility power system disconnects
- J. Six 300-gallon day tanks with dual pumps, two aboveground fuel storage tanks and all related fuel pumps and piping.
- K. Veeder-root fuel monitoring system (this includes ordering and replacing paper as needed)
- L. Hydrogen Gas Detector, located in the UPS Battery Room (note – limited to testing only)
- M. Cummins power command center, which accesses the on-board power command system of each of the generators #1 through #4.
- N. Two Cummins (Generators #5 and #6) 2250kW diesel generator set Model DQKAF-1332787 and DQKAF-1332805 (with on-board Power Command digital paralleling system) with lead-acid starting batteries, battery charger, generator enclosure and other attached components including dampers. Also, generators are controlled by Square D switch gear with Programmable Logic Controllers (PLC).
- O. One Cummins Power Command Paralleling Digital Master Control Station (MCS) and remote computer (equipment located in room 160D).
- P. Facility Electrical Infrastructure (FEI) including electrical feeders, breakers, Data Center CLP Electrical Panels, Electrical Feeder/Electrical Breakers to Power Distribution Units/Remote Power Panels (PDUs/RPPs), Electrical Panel PBCCM in Rm. 160B, and miscellaneous switch gear.

4.3 GENERATOR WARRANTY SUPPORT

Contractor maintenance for Cummins generators under warranty shall be performed in accordance with the Cummins five (5) year Warranty as specified in Attachment 1 “Cummins Power Generation Warranty Statements, Generator Sets, Commercial Standby Extended Warranty Statements” throughout the warranty period. The

AITC EDGS REPAIRS & PARTS CONTRACT TAC-16-23826

Contractor shall ensure all replacement parts are Cummins Original Equipment Manufacturer (OEM) parts. Generator warranty build dates at the time of this writing are:

- Generator #5: 8/1/13
- Generator #6: 8/5/13

4.4 MASTER CONTROL STATIONS (MCS) SUPPORT

The MCS contains Cummins developed software that allows a VA technician to monitor the health of each of the generators from the MCS position. In addition, it is used to run the tests (e.g., weekly test). Further, the MCS performs automatic transfer (switchover) during a power outage to prevent interruption of electrical services to maintain data center functions.

The MCS software communicates to the EDGS via a Cummins proprietary protocol. Failure to maintain the MCS may result in the inability to monitor or run required tests, which would place the generators at greater risk of power outages.

Prior to performing any work on the MCS, the Contractor shall consult with Cummins to confirm that any MCS work is performed in a manner (i.e., Cummins performs software upgrade) that will not result in the proprietary software being compromised. The Contractor shall consult with the COR for VA approval before proceeding with any MCS maintenance or repair work e.g., software patch. The Contractor shall ensure quarterly preventive maintenance is performed on the MCS and software system. The quarterly preventive maintenance work shall be captured (test results, repair, etc.) and provided in a MCS Preventive Maintenance Inspection Report.

Deliverable:

- A. MCS Preventive Maintenance Inspection Report

4.5 GENERATOR MAINTENANCE

The Contractor shall perform a level of maintenance and load testing on the AITC EDGS generators over the course of the period of performance as specified in the following subparagraphs to ensure that the generators are available and capable of performing at required load levels. In addition, the Contractor maintenance shall include FEI equipment. All maintenance and repair/replacement work shall be performed by stationary diesel generator repair/maintenance certified technicians.

The following subsections define the type of maintenance, as well as the frequency of the functions to be performed by the Contractor. In addition, the Contractor shall record the status of the generators based on the maintenance performed. The Contractor shall document the maintenance activity performed in the following subtasks in a Maintenance Report.

Details regarding Contractor maintenance activities, scheduling of maintenance tasks with the VA, and identification of specific generators to be maintained shall be specified in individual TOs.

AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826

Deliverable:

- A. Maintenance Report

4.5.1 PREVENTIVE MAINTENANCE

The Contractor shall perform annual generator maintenance activities prior to performing the Load Tests detailed in Sections 4.6.2, 4.6.3, and 4.6.4, consisting of:

- A. Oil
 - 1. Drained and Replaced with New Oil and Dispose of old oil off-site.
- B. Replacement of Filters (Dispose of old filters off-site)
 - 1. Fuel Filter
 - 2. Air Filters
 - 3. Water Filters
 - 4. Oil Filters

The Contractor shall capture all the work performed (e.g., date oil and filter replaced on which generator) in the Maintenance Report. The Contractor shall comply with Environment Protection Agency (EPA) regulations. Hazardous Waste Recycling Regulations can be found

at: <http://www3.epa.gov/epawaste/hazard/recycling/regulations.htm>

4.5.2 ODD-YEAR MAINTENANCE

In addition to the tasks above, on years ending in an odd number (e.g. 2017), the Contractor shall perform the following odd-year tasks:

- A. Replace all lead acid start batteries.
- B. Drain all coolant and replace with fresh, de-ionized water and new anti-freeze to provide protection down to -30 degree Fahrenheit. Contractor shall dispose of old coolant off-site.
- C. Replace all belts, hoses and hose clamps.

The Contractor shall include any Odd-Year Maintenance activities in the Maintenance Report. The Contractor shall comply with Environment Protection Agency (EPA) regulations. Hazardous Waste Recycling Regulations can be found

at: <http://www3.epa.gov/epawaste/hazard/recycling/regulations.htm>

4.6 GENERATOR TESTING

The Contractor shall perform several types of tests on the AITC EDGS generators over the course of the period of performance to ensure that the generators are available and capable of performing at required load levels. The following subsections define the type of testing and the frequency of the testing the Contractor shall be responsible to perform. In addition, the Contractor shall record the results of the testing and submit them as specified in the following subsections.

**AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826**

4.6.1 WEEKLY GENERATOR TESTING

On a weekly basis and in coordination with the COR, the Contractor shall perform weekly non-load generators run testing on Thursdays from 4:30pm CT to 6:00pm CT. The Contractor shall perform a 15 minute 'no-load' test of each generator system (do not interrupt power to the critical load) and document all findings, repairs and replacements in an Inspection Report. The inspection reporting requirements of this PWS must be completed for each individual generator; therefore, each generator shall have its own Inspection Report. The Contractor shall arrive at the AITC every Thursday between 4:30 PM CT and 4:45 PM CT to perform this requirement. Prior to commencing, the Contractor shall send out a text message from the Power Command PC to VA-AITC personnel notifying them at the start of the weekly testing. At the conclusion of the weekly testing, the Contractor shall send a text message from the Power Command PC to VA-AITC personnel notifying them that weekly testing has been completed and then clear all messages.

Activities shall be performed in accordance with the requirements included in the PWS and NFPA 110, "Standard for Emergency and Standby Power Systems". The Contractor shall add oil and coolant to the generator system as necessary and add water to the starting batteries as necessary.

The Contractor shall include in the Inspection Report a list of failed components and whether the components were replaced or repaired. The Contractor shall provide in the Inspection Report at a minimum the following data elements for each generator:

- A. System Operation Checks/Generator Run Test without Load in paralleling system
 1. Visual inspection of Generator enclosures (Good, Fair or Poor)
 2. Visual Inspection of Transfer Switch/Switch Gear Test (Good, Fair or Poor)
 3. Visual Inspection of Transfer Switch/Switch Gear Lamps (Good or Bad)
 4. Visual Inspection Transfer Switch/Switch Gear Housing (Good, Fair or Poor)
 5. Generator Performance in Accordance With Standard Generator Operations (Good, Fair or Poor)
 6. Visual inspection Control Panel (Good, Fair or Poor)
 7. Record Time Generator Takes to Come On-Line – From initiation of test to closing of output circuit breaker.
- B. Visual Inspection Damper Operations and Controls for Openings and Closings (Repair as necessary) (Good, Fair or Poor)
- C. Battery Checks:
 1. Record Condition of starting batteries (Readings in Volts and Amps and rated as Good, Fair or Poor)
 2. Record Float Charge (Pre-Start Readings in Volts and Amps and rated as Good, Fair or Poor)
 3. Record Alternator Engine (A/T) While Generator is Running (Readings in Volts and Amps and rated as Good, Fair or Poor)
 4. Terminals (Good, Fair or Poor)
 5. Record Water Level (If Applicable) (Full or Low), add as required
 6. Load Test (During Generator Engine Cranking) (Readings in Volts and Amps and rated as Good, Fair or Poor)

**AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826**

7. Record Specific Gravity (If Applicable) (Good, Fair or Poor)
8. Terminals (Good, Fair or Poor)
9. Battery Racks Cleaned (Yes/No)
- D. Fuel System Checks:
 1. Replace Filters as Required (Good, Fair or Poor)
 2. Fuel Separator (Good, Fair or Poor)
 3. Lines (Good, Minor or Moderate)
 4. Solenoid (Good, Fair or Poor)
 5. Record and Printout Fuel Tanks Levels (replace paper as necessary)
(Reading in Gallons)
 6. Pump (Good, Fair or Poor)
 7. Visual Inspection of Crankcase Vent Tube Basin (Replace and repair as
necessary (Good, Fair or Poor)
- E. Cooling System/Block Heater Checks:
 1. Filters (Good, Fair or Poor)
 2. Heaters (Good, Fair or Poor)
 3. Leaks (Good, Minor or Moderate)
 4. Sample Taken (Yes/No and provide sample resolute)
 5. Level (Full or Low), add as required
 6. Hoses (Good, Fair or Poor)
 7. Belts (Good, Fair or Poor)
 8. Diesel Coolant Additive (DCA) (Yes/No)
- F. Lubrication System Checks:
 1. Level (Full or Low), add as required
 2. Leaks (Good, Minor or Moderate)
 3. Filter (Good, Fair or Poor)
 4. Condition (Good, Fair or Poor)
 5. Sample Taken (Yes/No and provide sample resolute)
- G. Ignition System Checks:
 1. Diesel Fuel Injection (Good, Fair or Poor)
- H. Exhaust System Checks:
 1. Leaks (Good, Minor or Moderate)
 2. Turbo Charger (Good, Fair or Poor)
 3. Condensation (Yes/No)
 4. Wet Stack (Yes/No)
 5. Flex Pipe (Good, Fair or Poor)
 6. Rain Cap (Good, Fair or Poor)
- I. Gauge Readings
 1. Record AC leg Voltages
 - i. AB
 - ii. BC
 - iii. CA
 - iv. AN
 - v. BN
 - vi. CN
 2. Record AC Amps

AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826

- i. A Φ
 - ii. B Φ
 - iii. C Φ
- 3. Record Frequency (Hz)
- 4. Record Oil Pressure (Pounds Per Square Inch [PSI])
- 5. Record Engine Temperature (Fahrenheit)
- 6. Record Hour Meter (Hours)
- J. Air Filter Checks:
 - 1. Element (Good, Fair or Poor)
 - 2. Restrictions (Yes/No)
- K. Hydrogen Gas Detector Test (**Monthly**)
 - 1. Verification that Alarm is Working; Use Test Button (Yes/No)
- L. Cleaning
 - 1. Generators (Yes/No)
 - 2. Pads (Yes/No)
 - 3. Fuel pipes (Yes/No)
 - 4. Paint touch up (Yes/No)
 - 5. Battery racks (Yes/No)
 - 6. Starting battery tops (Yes/No)
- M. Final View Checks:
 - 1. Unit Housing (Good, Fair or Poor)
 - 2. Decal (Good, Fair or Poor)
 - 3. System Auto Ready (Yes/No)
 - 4. Circuit Breaker On (Yes/No)
 - 5. Automatic Transfer Switch (ATS) in Auto (Yes/No)
 - 6. Power Command PC Time Verified (Yes/No)
 - 7. All Indicator Lamps Illuminated (Good or Bad)
 - 8. Activate Test Button on All Diesel Fuel Pumps (Yes/No)
 - 9. Repair All Observed Leaks and Seepage (Yes/No)
 - 10. Door Closed (Yes/No)

Items requiring corrective action for weekly activities (do not require COR approval):

- A. Leaks
- B. Replace Dead or Dull Lamps
- C. Paint Touch-Up
- D. Tightening of bolts and clamps
- E. Closed Door
- F. Tighten Battery Cables
- G. Top off Coolant
- H. Top off Oil
- I. Lubrication

The Contractor shall record the estimated labor and cost of any parts needing to be replaced (e.g., oil gasket, FEL, feeder, breaker, etc.) in the Estimate of Repair Cost Report in accordance with each TO. Upon review and approval by the COR the

**AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826**

Contractor shall proceed with the repair in accordance with Section 4.7 Emergency Repairs/Non-Emergency Repairs.

Deliverables:

- A. Inspection Report
- B. Estimate of Repair Cost Report

4.6.2 EARLY-YEAR and MID-YEAR LOAD TEST

The Contractor shall perform a four hour load test for all generators consisting of the following tasks:

- A. Record the following parameters for generator and switchgear (DMS #1 and #2 system) (each phase of output) every 15 minutes during the full-load test: voltage, current, frequency, oil pressure, oil temperature, coolant temperature as a minimum. Also record fuel levels of day tanks and main tank every 15 minutes.
- B. Inspect emergency generators system 15 minutes after shutdown of generators to ensure there are no leaks, etc. Repair all leaks observed.
- C. Remove all materials from the site upon completion of each maintenance activity.
- D. Verify that all switches, circuit breakers, disconnect, etc. are in their proper position for automatic operation of the emergency diesel generator system.

For Generators #1, #2, #3 and #4, the load test shall consist of using building live load via transfer switches under direction of COR/VA facilities engineers.

For Generators #5 and #6, the Contractor shall follow the same procedures listed above, except for the contractor-provided load bank will be utilized in lieu of building load bank. The Contractor shall prepare for load testing as follows:

1. The Contractor shall provide a rented 4,000 kW Load Bank System (resistive and reactive).
2. The load bank will be connected to the 5,000 A load bank Circuit Breaker T11 installed in GPSG #1 for load bank.
3. The load bank 4,000 kW load will be added in stages until each generator is loaded to 4,000 kW.
4. All necessary wiring for load bank testing with proper terminal connections shall be provided. The quantity of lugs based on parallel cables sized for generator capacity shall be provided for connection to the portable load bank.
5. Perform annual full-load test using load bank in coordination with the COR. Response to all alarms on the generator and GPSG #1 shall be required by qualified technicians during this test. Contractor will repair any components that fail during the test that is supplied with the load bank system.
6. The load bank shall be connected a minimum of 30 minutes prior to the scheduled start of the test. Inspect emergency generator system to ensure it is ready for the test to begin. Setup the monitoring equipment for trending all points during generator load test, download to disk, and provide a printout at the next weekly inspection.

AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826

4.6.3 ANNUAL EARLY-YEAR LOAD TEST

The Contractor shall provide annual early-year load testing. Prior to an Annual Early-Year Load Test, the Contractor shall perform Generator Maintenance coordinated with the COR. The Generator Maintenance, Odd-Year maintenance (if applicable), and Fluid Analysis sampling shall be followed by the Load Test with the Infrared Scanning Test during the first and last hour of testing and inspection activities throughout the load testing. Included in this task is the requirement to perform the task defined in PWS Section 4.6.1, Weekly Generator Testing.

The Contractor shall perform the following four (4) hour annual load test, beginning on Saturday at midnight, using available building load during the month of April. This date/time may change and is dependent on approval by the COR. Typically, the Contractor arrives at the AITC between 11:00 PM CT and 11:15 PM CT to perform this requirement. The test shall be completed in accordance with the Annual Early-Year Load Test Reporting Requirements and the NFPA 110. The Contractor shall respond to all alarms on the EDGS and ATSS during this test, and repair or replace any components that fail during the test.

The Contractor shall receive COR approval before initiating repairs. The Contractor shall remove all materials from the site upon completion of this task. The Contractor shall perform the Annual Early-Year Load Test to include at a minimum the following data elements recorded every 15 minutes for each generator during the 4 hour load test:

- A. Systems Operation Checks for Generators and ATS
 1. Record Voltage
 2. Record Kilowatts (kW)
 3. Record Current (Amps)
 4. Record Frequency (Hz)
 5. Record Oil Pressure (PSI)
 6. Record Oil Temperature (Fahrenheit)
 7. Record Coolant Temperature (Fahrenheit)
 8. Record Fuel Levels of Day Tanks (Number of Gallons)
 9. Record Fuel Levels of Main Tanks (Number of Gallons)
 10. Record Percentage of Generator Rating (% of Load)

- B. Post Load Checks (Conducted 15 minutes after shutdown of generators):
 1. Repair Leaks as observed
 2. Clean and Lubricate All Exhaust Flappers
 3. Verify that all switches, circuit breakers, disconnect, etc. are in their proper position for automatic operation of the emergency diesel generator system.
 4. Reset the Power Command trend log upon completion of the testing.

The Contractor shall record the observations made during generator inspections (e.g., leaking gasket) in the Load Test Generator Inspection Report.

AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826

The Contractor shall record approximately every 30 minutes the results of each load test in the Annual Early-Year Load Test Report.

The Contractor shall record the estimated labor and cost of any parts that may need to be replaced (e.g., oil gasket) in the Estimate of Repair Cost Report as specified above in Section 4.6.1. Upon review and approval by the COR the Contractor shall proceed with the repair in accordance with Section 4.7 Emergency Repairs/Non-Emergency Repairs.

The Contractor shall perform a fluid lab analysis and infrared scanning as specified in the following subsections.

Deliverables:

- A. Load Test Generator Inspection Report
- B. Annual Early-Year Load Test Report

4.6.3.1 FLUID LAB ANALYSIS

The Contractor shall provide a lab analysis of the crankcase oil and cooling water condition during maintenance phase prior to load testing. The Contractor shall record the analysis findings in a Crankcase Oil and Coolant Lab Analysis Test Result Report.

Deliverable:

- A. Crankcase Oil and Coolant Lab Analysis Test Result Report

4.6.3.2 INFRARED SCANNING

The Contractor shall provide infrared scanning. Two Infrared (IR) Scanning Tests may be required along with the recording of the test results. The first IR scan shall be performed during the first hour of a load test. The second test shall be performed during the last hour of a load test. IR Scanning is typically performed to detect loose electrical wire connections, switch gears and ATSS and correct as necessary. The Contractor shall record the analysis findings in an IR Scanning Test Result Report.

Deliverable:

- A. IR Scanning Test Result Report

4.6.4 ANNUAL MID-YEAR LOAD TEST

The Contractor shall perform the following Annual Mid-Year Load Test for each generator during the projected month of October. This date/time may change and is dependent on approval by the COR. This annual task shall be coordinated with the COR a month in advance. The Contractor shall arrive at the AITC between 11:00 PM CT and 11:15 PM CT to perform this requirement. The Contractor shall respond to all

AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826

alarms on the EDGS and ATSS during this test, and repair or replace any components that fail during the test. The Contractor must receive approval from the COR before initiating repairs.

The reporting requirements must be completed for each individual generator that the Annual Mid-year Load test has been performed and included in the Load Test Generator Inspection Report.

Included in this task is the requirement to perform the same set of tasks defined in PWS Section 4.6.1, Weekly Generator Testing while under load. The Contractor shall provide a summary of the activities performed in the Annual Mid-Year Load Test Report, to include a list of all failed components, indicating whether those parts will be replaced or repaired. In the Annual Mid-Year Load Test Report, the Contractor shall at a minimum, include a recording of the following data elements every 15 minutes for each generator during the 4 hour load test:

- A. Systems Operation Checks for Generators and ATS
 - 1. Record Voltage
 - 2. Record Kilowatts (kW)
 - 3. Record Current (Amps)
 - 4. Record Frequency (Hz)
 - 5. Record Oil Pressure (PSI)
 - 6. Record Oil Temperature (Fahrenheit)
 - 7. Record Coolant Temperature (Fahrenheit)
 - 8. Record Fuel Levels of Day Tanks (Number of Gallons)
 - 9. Record Fuel Levels of Main Tanks (Number of Gallons)
 - 10. Record Percentage of Generator Rating (% of Load)
- B. Post Load Checks (Conducted 15 minutes after shutdown of generators):
 - 1. Repair Leaks as observed
 - 2. Clean and Lubricate All Exhaust Flappers
 - 3. Verify that all switches, circuit breakers, disconnect, etc. are in their proper position for automatic operation of the emergency diesel generator system.

The Contractor shall reset the Power Command trend log upon completion of the testing.

4.7 EMERGENCY REPAIRS/NON-EMERGENCY REPAIRS (T&M)

The Contractor provided emergency and non-emergency repairs shall be performed after receiving an alarm notification. The Contractor shall contact the VA within 30 minutes of receiving an alarm notification. The Contractor shall be on site within one (1) hour for any emergency maintenance situation. The one (1) hour response time starts when the call is placed and ends when the technician/mechanic arrives on-site. The Contractor repairs shall be as follows:

**AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826**

- A. Emergency Repairs: Activities requiring immediate action to repair failed equipment which present an imminent risk to operations to the data center. Emergency repairs shall be required whenever any generator is not fully operational. The maintenance on the EDGS, ATSSs, and FEI shall be performed in accordance with the requirements included in the PWS and NFPA 110.
- B. Non-Emergency Repairs: Activities requiring immediate action to repair failed equipment and which do not present an imminent risk to operations to the data center (e.g. leaky failed fuel pump gasket and all other generators are still able to operate). Parts are to be delivered within 30 days from day of notification of issue to the COR.

Replacement parts required to perform emergency and non-emergency repairs, to include the FEI, shall be provided by the Contractor in case of failure.

Upon Contractor response and identification of required repair, the Contractor shall record the estimated labor and cost of any parts needing to be replaced in the Emergency/Non-Emergency Estimate of Repair Cost Report. Upon review and approval by the COR the Contractor shall proceed with the repair. Following resolution, the Contractor shall record the failure type, cause, and corrective action taken for each issue in a Corrective Action Report. Historically, there have been between 1 and 3 reports issued annually.

Deliverable:

- A. Emergency/Non-Emergency Estimate of Repair Cost Report
- B. Corrective Action Report

5.0 DELIVERABLES

5.1 PRODUCTS

All products shall be delivered to the Government locations and accepted by authorized Government personnel as specified in the individual TO. Inspection and acceptance criteria shall be specifically identified in each TO. The COR shall be notified of any discrepancies found during acceptance inspection upon identification.

5.2 DATA

The preliminary and final deliverables and all associated working documents and other material deemed relevant by the Government which has been generated by the Contractor in performance are the exclusive property of the Government or as specified in the individual TO. Request for deviation shall be approved by the CO. Data rights for all final deliverables and working papers shall be in accordance with the individual TO.

**AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826**

6.0 SECURITY AND PRIVACY

6.1 INFORMATION SECURITY AND PRIVACY SECURITY REQUIREMENTS

The Contractor shall comply with the VA security requirements in accordance with (IAW) VA Handbook 6500.6 "Contract Security" and Addendum A of this document. VA Handbook 6500.6 Appendix C "VA Information Systems Security/Privacy Language for Inclusion into Contracts, As Appropriate" is included within this document as Addendum B. Addendum B may be tailored at the TO level.

6.2 POSITION/TASK RISK DESIGNATION LEVEL(S)

Position Sensitivity	Background Investigation (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A)
Low / Tier 1	Tier 1 / National Agency Check with Written Inquiries (NACI) A Tier 1/NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.
Moderate / Tier 2	Tier 2 / Moderate Background Investigation (MBI) A Tier 2/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 / Tier 4	Tier 4 / Background Investigation (BI) A Tier 4/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 PWS are:

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low / NACI	Tier 2 / Moderate / MBI	Tier 4 / High / BI
--------------------	---------------------------	--------------------------------	---------------------------

**AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826**

Task Number	Tier1 / Low / NACI	Tier 2 / Moderate / MBI	Tier 4 / High / BI
4.1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4.2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4.3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4.4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4.5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4.6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4.7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4.8	<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.

6.3 FACILITY/RESOURCE PROVISIONS

Not Applicable.

6.4 BADGES

Employees working at a Government facility shall display, on their person, a Government-provided identification badge, that shall include the full name of the employee and the legal name under which the Contractor is operating. It is the responsibility of the Contractor to request and obtain badges from the Government prior to the first workday of any Contractor employee. The Contractor shall return all badges to the Government program manager, or designee, on the same day an individual's employment is terminated and upon termination of the contract. The Contractor shall notify the Government program manager, or designee, immediately of any lost badges.

7.0 REPORTING AND MEETING REQUIREMENTS

7.1 REPORTING REQUIREMENTS

The deliverables defined above may be required for each TO.

7.2 MEETINGS AND REVIEWS

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

7.2.1 PROJECT OFFICE INITIAL PROGRAM REVIEW (IPR)

The COR shall host an IPR within 30 days after contract award to review the PWS, business policies, and procedures, and introduce personnel.

**AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826**

7.2.2 POST-AWARD CONFERENCES

The Government intends to convene a Post-Award Conference with the awardee within 30 days after contract award. The CO shall notify the Contractor of a specific date, location and agenda within 15 days after contract award.

**AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826**

**ADDENDUM B- VA INFORMATION AND INFORMATION SYSTEM SECURITY /
PRIVACY LANGUAGE**

**VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE
VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010**

B1. GENERAL

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

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

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

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

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

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates (e.g. Business Associate Agreement, Section 3G), 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.

AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826

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

a. 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).

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

c. 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.

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

AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826

e. 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.

f. 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.

g. 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 1600.05, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

h. 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.

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

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

k. 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.

l. 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

AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826

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

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

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

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

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

e. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

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

g. The Contractor/Subcontractor agrees to:

AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826

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

- a) The Systems of Records (SOR); and
- b) The design, development, or operation work that the Contractor/Subcontractor is to perform;

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

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

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

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

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

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

i. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as "Systems"),

AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826

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

j. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, but in no event longer than ____ days.

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

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

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

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA's network involving VA information must be in accordance with the TIC Reference Architecture and reviewed and approved by VA prior to implementation.

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

AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826

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

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

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

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

AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826

Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

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

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

- 1) Vendor must accept the system without the drive;
- 2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or
- 3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.
- 4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;
 - a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and
 - b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.
 - c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

B6. SECURITY INCIDENT INVESTIGATION

AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826

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

AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826

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;

AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826

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

B8. SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the Contractor under the clauses contained within the contract. With 10 working-days notice, at the request of the Government, the Contractor must fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

B9. TRAINING

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

1) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* course (TMS #10176) and complete this required privacy and security training annually; Sign and acknowledge (electronically through TMS #10176) 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 any additional cyber security or privacy training, as required for VA personnel with equivalent information system access *[to be defined by the VA program official and provided to the contracting officer for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]*

AITC EDGS REPAIRS & PARTS CONTRACT
TAC-16-23826

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 electronically 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.