



## **PERFORMANCE WORK STATEMENT (PWS) DEPARTMENT OF VETERANS AFFAIRS**

**Veterans Health Administration (VHA)  
Veterans Affairs Medical Center (VAMC)**

**Maintenance, Repairs, and Upgrades for the VA Freight Transportation System**

**Date: July 11, 2017  
TAC-18-43713  
PWS Version Number: 5.1**

### **Request for Information (RFI)**

**\*\*This posting is not a formal request for quote, but rather a market research request to determine if there are viable sources to provide the above requirement.\*\***

# Maintenance, Repairs, Upgrades for the VA Freight Transportation System

TAC Number: TAC-18-43713

## Contents

1.0	BACKGROUND.....	3
2.0	APPLICABLE DOCUMENTS.....	3
3.0	SCOPE OF WORK.....	4
4.0	PERFORMANCE DETAILS.....	5
4.1	PERFORMANCE PERIOD.....	5
4.2	PLACE OF PERFORMANCE.....	5
4.3	TRAVEL.....	5
5.0	SPECIFIC TASKS AND DELIVERABLES.....	6
5.1	KICKOFF MEETING.....	6
5.1.1	REPORTING REQUIREMENTS.....	6
5.2	VATLC APPLICATION TECHNICAL SUPPORT.....	7
5.2.1	VATLC APPLICATIONS UPGRADE and MAINTENANCE.....	7
5.2.2	SERVICE RESPONSE TIMEFRAMES.....	8
6.0	GENERAL REQUIREMENTS.....	8
6.1	ENTERPRISE AND IT FRAMEWORK.....	8
6.2	SECURITY AND PRIVACY REQUIREMENTS.....	8
6.2.1	POSITION/TASK RISK DESIGNATION LEVEL(S).....	8
6.2.2	CONTRACTOR PERSONNEL SECURITY REQUIREMENTS.....	9
6.3	METHOD AND DISTRIBUTION OF DELIVERABLES.....	10
6.4	PERFORMANCE METRICS.....	10
6.5	FACILITY/RESOURCE PROVISIONS.....	12
	ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED.....	13
	ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM	
	SECURITY/PRIVACY LANGUAGE.....	21
	POINTS OF CONTACT.....	27

# **Maintenance, Repairs, Upgrades for the VA Freight Transportation System**

## **TAC Number: TAC-18-43713**

### **1.0 BACKGROUND**

Department of Veterans Affairs, Transportation and Logistics Center (VATLC) manages and reports on the delivery, timeliness, and costs to transport goods throughout the national VA infrastructure. The VATLC is functionally divided into two primary functions: (1) traffic management and (2) administrative support for network/client systems and database maintenance.

The database application Sesame which supports General Freight and Operation New Hope Application for both VATLC and VA's Homeless Veterans Clothing Distribution Program. This requirement is for software maintenance of General Freight and Operation New Hope applications. This software is currently being used by VATLC. This requirements is for periodic upgrading of the software, patches to the software, modifications, additional reporting capabilities, software support, and repairs. The current software resides on a server continuously monitored by the VA Central Office (VACO) network at the Washington, DC and is also accessed from remote locations in Chicago, Illinois and Hillsborough, New Jersey. Access to Help Desk support will be from 6 AM to 8 PM EST Monday through Friday.

The VATLC users are VA Traffic Managers responsible for the timely and cost-effective transport of supplies and equipment throughout the VA infrastructure, commercial vendors and other government agencies. The current software supports the business functions listed below:

- Shipping and delivering supplies and equipment employing Transportation Service Providers (TSPs).
- Tracking freight, booking ocean cargo, obtaining air transport, and negotiating/selecting "best value" carrier rates.
- Preparation of warehouse inventories and bills of lading and ocean shipment manifests.
- Routing and monitoring shipments.
- Uploading and managing freight rates.
- Preparation of shipping documents.
- Report generation, estimating freight charges.
- Auditing and tracking freight bills/invoice payments.

### **2.0 APPLICABLE DOCUMENTS**

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

1. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2009"
2. FIPS Pub 2012, "Personal Identity Verification of Federal Employees and Contractors," September 2013
3. 10 U.S.C. § 2224, "Defense Information Assurance Program"
4. Software Engineering Institute, Software Acquisition Capability Maturity Modeling (SA CMM) Level 2 procedures and processes
5. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
6. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"

## **Maintenance, Repairs, Upgrades for the VA Freight Transportation System**

TAC Number: **TAC-18-43713**

7. Department of Veterans Affairs (VA) Directive 0710, "Personnel Security and Suitability Program," May 2, 2016
8. VA Directive 6102, "Internet/Intranet Services," July 15, 2008
9. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," March 2, 2017
10. OMB Circular A-130, "Management of Federal Information Resources," July 28, 2016
11. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
12. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
13. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
14. Homeland Security Presidential Directive (12) (HSPD-12)
15. VA Directive 6500, "Information Security Program," September 20, 2012
16. VA Handbook 6500, "Information Security Program," March 10, 2015
17. VA Handbook 6500.1, "Electronic Media Sanitization," November 3, 2008.
18. VA Handbook 6500.2, "Management of Security and Privacy Incidents," July 28, 2016.
19. VA Handbook 6500.3, "Certification and Accreditation of VA Information Systems," February 3, 2014.
20. VA Handbook, 6500.5, Incorporating Security and Privacy in System Development Lifecycle, February 3, 2014.
21. VA Handbook 6500.6, "Contract Security," March 12, 2010
22. Project Management Accountability System (PMAS) portal (reference PWS References -Technical Library at <https://www.voa.va.gov/>)
23. OI&T 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, OI&T ProPath takes precedence over other processes or methodologies.
24. Technical Reference Model (TRM) (reference at <http://www.ea.oit.va.gov/Technology.asp>)
25. National Institute Standards and Technology (NIST) Special Publications
26. VA Directive 6508, VA Implementation of Privacy Threshold Analysis and Privacy Impact Assessment, October 15, 2014
27. VA Directive 6300, Records Management, July 10, 2012
28. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010

### **3.0 SCOPE OF WORK**

The Contractor shall provide technical support and maintenance services for General Freight and Operation New Hope applications. Application maintenance shall include all production fixes, functional enhancements, software upgrades and modifications to include installing the most recent Lantica, Inc, Sesame software versions.

# Maintenance, Repairs, Upgrades for the VA Freight Transportation System

TAC Number: TAC-18-43713

## 4.0 PERFORMANCE DETAILS

### 4.1 PERFORMANCE PERIOD

The period of performance shall be twelve (12) months with four (4) twelve (12) month options for continued service. The Contractor shall continue to provide technical support and maintenance services to the VATLC in each option period. The support shall include all tasks outlined in sections 5.1 to 5.2.3.

With the exception of Emergency Maintenance Calls, the Contractor must plan downtime, upgrades, and any other disruption to the VATLC to occur during non-duty hours (between 3:30 PM and 6:59 AM, EST Monday through Friday). If this is not possible, the Contractor shall provide written advance notice and obtain approval by the Contracting Officer's Representative (COR) before system shut down can occur.

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

There are ten (10) Federal holidays set by law (USC Title 5 Section 6103) that the 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 remotely at Contractor's facilities.

### 4.3 TRAVEL

Travel will not be required under this effort

## **Maintenance, Repairs, Upgrades for the VA Freight Transportation System**

TAC Number: **TAC-18-43713**

### **5.0 SPECIFIC TASKS AND DELIVERABLES**

The Contractor shall perform the following:

#### **5.1 KICKOFF MEETING**

The Contractor shall conduct a project kick-off meeting within two (2) weeks of award to introduce the Government team to the Contractor's overall operating plans and approach to this work. The Kick-off Meeting shall be via teleconference. The Contractor shall deliver a Kick-Off Meeting Agenda and Kick-Off Meeting Minutes identifying all the discussion points, agreements and action items. .

##### **Deliverables:**

- A. Kick-off Meeting Agenda
- B. Kick-off Meeting Minutes

#### **5.1.1 REPORTING REQUIREMENTS**

The Contractor shall provide the COR with Monthly Progress Reports in electronic form in Microsoft Word and Project formats. The report shall include detailed instructions/explanations for each required data element, to ensure that data is accurate and consistent. These reports shall reflect data as of the last day of the preceding month.

The Monthly Progress Reports shall cover all work completed during the reporting period. The report shall 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 report 100% accuracy for status of the task completion. The Contractor shall monitor performance to ensure compliance with planned functionality and report any deviations. It is expected that the Contractor will keep in communication with the VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

The Contractor shall provide a weekly update to the COR to be communicated through email and / or telephone conferences, or face to face meetings. The weekly conference calls will take place between the Contractor and the COR to review progress and resolve design issues. The contractor shall provide Monthly Progress Reports to the COR with a copy to the CO. Reports shall be submitted via email. This report shall contain the following information:

Contract number  
Contractor name  
Period covered by report  
Provide a summary description of activities and accomplishments during the reporting period.

Description of problems and issues encountered during the report period.

## **Maintenance, Repairs, Upgrades for the VA Freight Transportation System**

TAC Number: **TAC-18-43713**

Provide a description of work to be accomplished during the following reporting period and the “value added”.

Provide the status of open problems or issues identified in previous report(s).

### **Deliverable:**

A. Monthly Progress Report

## **5.2 VATLC APPLICATION TECHNICAL SUPPORT**

### **5.2.1 VATLC APPLICATIONS UPGRADE and MAINTENANCE**

The Contractor shall provide technical support and maintenance of each VATLC application (General Freight and Operation New Hope). Software maintenance shall include all production fixes, functional enhancements to General Freight and Operation New Hope, application upgrades and modifications to include the installation of the most recent Lantica, Incorporated Sesame software versions. All disruptions to on-going service shall be coordinated through the COR and appropriate VA facility staff, with the concurrence of the COR to ensure minimum interruption or impacts to on-going VA services/functions. The COR shall develop a methodology for acceptance testing of completed work. The plan shall be used for testing and acceptance of the system and include sufficient tests to validate the functional capabilities of the services. The Contractor shall document all of the VATLC software modifications performed by the Contractor. In the event that the application modification process inappropriately affected the functionality of other existing applications, the Contractor shall repair the affected function at no cost to the VA. The Contractor shall ensure and validate that the activities involving new upgrades or modification of VATLC applications will not affect normal business performance VATLC System.

The Contractor shall provide remote technical support for the VATLC applications to VA’s Centralized Transportation Centers (CTC) in Washington, DC; Hillsborough, NJ; and Hines, IL; Martinsburg, WV.

The Contractor shall provide updates to VATLC applications training manuals with detailed step-by-step text and clear readable graphics screen shots. The Contractor shall also provide addendums to detail any source code to reflect changes made to basic programming in the current system.

### **Deliverables:**

- A. Updated Training Manual for General Freight & Operation New Hope Applications
- B. General Freight & Operation New Hope Applications: Process, Methodologies, Source Code

## Maintenance, Repairs, Upgrades for the VA Freight Transportation System

TAC Number: TAC-18-43713

### 5.2.2 SERVICE RESPONSE TIMEFRAMES

1. Helpdesk support, problem resolution, and bug fixes within 24 hours for issues critical to operation including emergency assistance to resolve access issues related to server operations and client application setup;
2. Respond within 72 hours for major user deficiencies. Major deficiencies are defined as a disruption of performance
4. Respond within 120 hours for minor deficiencies.

## 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 OI&T Technical Reference Model (One-VA TRM). One-VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. Architecture, Strategy, and Design (ASD) has overall responsibility for the One-VA TRM.

### 6.2 SECURITY AND PRIVACY REQUIREMENTS

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

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 Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	<input checked="" type="checkbox"/>	<input 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.



## **Maintenance, Repairs, Upgrades for the VA Freight Transportation System**

TAC Number: **TAC-18-43713**

### **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. 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 in accordance with the ProPath (PAL) template. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.
- c. The Contractor should coordinate with the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized. The Contractor shall bring their completed Security and Investigations Center (SIC) Fingerprint request form with them (see paragraph d.4. below) when getting fingerprints taken.
- d. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
  - 1) Optional Form 306
  - 2) Self-Certification of Continuous Service
  - 3) VA Form 0710
  - 4) Completed SIC Fingerprint Request Form
- e. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
- f. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via e-QIP).

## **Maintenance, Repairs, Upgrades for the VA Freight Transportation System**

TAC Number: **TAC-18-43713**

- g. 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.
- h. 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), completed training delineated in VA Handbook 6500.6 (Appendix C, Section 9), signed "Contractor Rules of Behavior", and with a valid, operational PIV credential for PIV-only logical access to VA's network. A PIV card credential can be issued once your SAC has been favorably adjudicated and your background investigation has been scheduled by OPM. 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 OPM.
- i. 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.
- j. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.
- k. Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

### **Deliverable:**

- A. Contractor Staff Roster

## **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 Levels of Performance associated with this effort.

**Maintenance, Repairs, Upgrades for the VA Freight Transportation System**  
**TAC Number: TAC-18-43713**

The Contractor must have a demonstrable focus on maintenance quality. The contractor shall follow strict guidelines for quality control. These guidelines will ensure the stability and reliability of the data, technology, and processes that compose the VATLC system. The contractor shall ensure that all components of the system comply with these guidelines. The contractor shall demonstrate quality control in terms of policy, processes and procedures. To the extent required, the contractor must provide a timely, systematic and accurate response to ad hoc requests. The contractor should strive to achieve industry level standard certifications in quality of all system components.

VATLC staff shall evaluate contractor performance and deliverables against the following criteria to determine final acceptance and completion of tasks.

<b>Performance Objective</b>	<b>Performance Standard</b>	<b>Acceptable Levels of Performance</b>
A. Technical / Quality of Product or Service	<ol style="list-style-type: none"><li>1. Demonstrates understanding of requirements</li><li>2. Efficient and effective in meeting requirements</li><li>3. Meets technical needs and mission requirements</li><li>4. Provides quality services/products</li></ol>	Satisfactory or higher
A1. Help Desk/Support Personnel	Helpdesk support, problem resolution, and bug fixes within 24 hours for issues critical to operation; within 72 hours for major user deficiencies; and within 120 hours for minor inconvenience	Deliverables are 100% on time and are not rejected on the initial submission
A2. VATLC System Operation	The VATLC System performance of reliability is 99.99% in each year of application upgrades and maintenance.	Total cumulative down time per year is less than .88 hours.

## Maintenance, Repairs, Upgrades for the VA Freight Transportation System

TAC Number: **TAC-18-43713**

B. Project Milestones and Schedule	<ol style="list-style-type: none"><li>1. Established milestones and project dates are met</li><li>2. Products completed, reviewed, delivered in accordance with the established schedule</li><li>3. Notifies customer in advance of potential problems</li></ol>	Satisfactory or higher
B1. User Guides, Training Manuals and other Documentation	Documentation provided meets the stated requirements in the PWS and are accurate, complete and easy to use with no grammar or mathematical errors.	100% for timeliness and 95% for accuracy as measured on a monthly basis
C. Cost & Staffing	<ol style="list-style-type: none"><li>1. Currency of expertise and staffing levels appropriate</li><li>2. Personnel possess necessary knowledge, skills and abilities to perform tasks</li></ol>	Satisfactory or higher
D. Management	<ol style="list-style-type: none"><li>1. Integration and coordination of all activities to execute effort</li></ol>	Satisfactory or higher

The COR 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 level of performance. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion. A Performance Based Service Assessment will be used by the COR in accordance with the QASP to assess Contractor performance.

### 6.5 FACILITY/RESOURCE PROVISIONS

The Government shall not provide office space, telephone service and system access. 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

## **Maintenance, Repairs, Upgrades for the VA Freight Transportation System**

TAC Number: **TAC-18-43713**

securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

VA may provide remote access to VA specific systems/network in accordance with VA Handbook 6500, which requires the use of a VA approved method to connect external equipment/systems to VA's network. Citrix Access Gateway (CAG) is the current and only VA approved method for remote access users when using or manipulating VA information for official VA Business. VA permits CAG remote access through approved Personally Owned Equipment (POE) and Other Equipment (OE) provided the equipment meets all applicable 6500 Handbook requirements for POE/OE. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved POE or OE. The Contractor shall provide proof to the COR for review and approval that their POE or OE meets the VA Handbook 6500 requirements and VA Handbook 6500.6 Appendix C, herein incorporated as Addendum B, before use. CAG authorized users shall not be permitted to copy, print or save any VA information accessed via CAG at any time. VA prohibits remote access to VA's network from non-North Atlantic Treaty Organization (NATO) countries. The exception to this are countries where VA has approved operations established (e.g. Philippines and South Korea). Exceptions are determined by the COR in coordination with the Information Security Officer (ISO) and Privacy Officer (PO).

This remote access may provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath (PAL), Primavera, and Remedy, including appropriate seat management and user licenses, depending upon the level of access granted. 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 VA Handbook 6500, 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. The Contractor shall ensure all work is performed in countries deemed not to pose a significant security risk. For detailed Security and Privacy Requirements (additional requirements of the contract consolidated into an addendum for easy reference) refer to ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED and ADDENDUM B - VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE.

### **ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED**

#### **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

## **Maintenance, Repairs, Upgrades for the VA Freight Transportation System**

TAC Number: **TAC-18-43713**

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, unless the connection uses FIPS 140-2 (or its successor) validated encryption, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COR, CO, the PM, 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**

## **Maintenance, Repairs, Upgrades for the VA Freight Transportation System**

TAC Number: **TAC-18-43713**

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](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](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.

#### **A3.1. 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: <https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards> and <http://www.section508.gov/content/learn/standards>. 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

## **Maintenance, Repairs, Upgrades for the VA Freight Transportation System**

TAC Number: **TAC-18-43713**

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

### **A3.2. Equivalent Facilitation**

Alternatively, offerors may propose products and services that provide equivalent facilitation, pursuant to Section 508, subpart A, §1194.5. Such offerors will be considered to have provided equivalent facilitation when the proposed deliverables result in substantially equivalent or greater access to and use of information for those with disabilities.

### **A3.3. Compatibility with Assistive Technology**

The Section 508 standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device. Section 508 requires that the EIT be compatible with such software and devices so that EIT can be accessible to and usable by individuals using assistive technology, including but not limited to screen readers, screen magnifiers, and speech recognition software.

### **A3.4. Acceptance and Acceptance Testing**

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the identified Section 508 standards' requirements for accessibility and must include final test results demonstrating Section 508 compliance.

Deliverables should meet applicable accessibility requirements and should not adversely affect accessibility features of existing EIT technologies. The Government reserves the right to independently test for Section 508 Compliance before delivery. The Contractor shall be able to demonstrate Section 508 Compliance upon delivery.

Automated test tools and manual techniques are used in the VA Section 508 compliance assessment. Additional information concerning tools and resources can be found at <http://www.section508.va.gov/section508/Resources.asp>.

#### **Deliverables:**

- A. Final Section 508 Compliance Test Results

### **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



## **Maintenance, Repairs, Upgrades for the VA Freight Transportation System**

TAC Number: **TAC-18-43713**

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 CO 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 CO 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

## **Maintenance, Repairs, Upgrades for the VA Freight Transportation System**

TAC Number: **TAC-18-43713**

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 CO.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
  - a. The use of "thumb drives" or any other medium for transport of information is expressly prohibited.
  - b. Controlled access to system and security software and documentation.
  - c. Recording, monitoring, and control of passwords and privileges.
  - d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
  - e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
  - f. Contractor PM and VA PM are informed within twenty-four (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

## **Maintenance, Repairs, Upgrades for the VA Freight Transportation System**

TAC Number: **TAC-18-43713**

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.

### **A6.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS**

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13693, "Planning for Federal Sustainability in the Next Decade", dated March 19, 2015; Executive Order 13221, "Energy-Efficient Standby Power Devices," dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, Federal Energy Management Program (FEMP) designated, low standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

The Contractor shall ensure that information technology products are procured and/or services are performed with products that meet and/or exceed ENERGY STAR, FEMP designated, low standby power, and EPEAT guidelines. The Contractor shall provide/use products that earn the ENERGY STAR label and meet the ENERGY STAR specifications for energy efficiency. Specifically, the Contractor shall:

1. Provide/use ENERGY STAR products, as specified at [www.energystar.gov/products](http://www.energystar.gov/products) (contains complete product specifications and updated lists of qualifying products).
2. Provide/use the purchasing specifications listed for FEMP designated products at [https://www4.eere.energy.gov/femp/requirements/laws\\_and\\_requirements/energy\\_star\\_and\\_femp\\_designated\\_products\\_procurement\\_requirements](https://www4.eere.energy.gov/femp/requirements/laws_and_requirements/energy_star_and_femp_designated_products_procurement_requirements). The Contractor shall use the low standby power products specified at <http://energy.gov/eere/femp/low-standby-power-products>.
3. Provide/use EPEAT registered products as specified at [www.epeat.net](http://www.epeat.net). At a minimum, the Contractor shall acquire EPEAT® Bronze registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified product lists. The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists.
4. The Contractor shall use these products to the maximum extent possible without jeopardizing the intended end use or detracting from the overall quality delivered to the end user.

## **Maintenance, Repairs, Upgrades for the VA Freight Transportation System**

TAC Number: **TAC-18-43713**

The following is a list of information technology products for which ENERGY STAR, FEMP designated, low standby power, and EPEAT registered products are available:

1. Computer Desktops, Laptops, Notebooks, Displays, Monitors, Integrated Desktop Computers, Workstation Desktops, Thin Clients, Disk Drives
2. Imaging Equipment (Printers, Copiers, Multi-Function Devices, Scanners, Fax Machines, Digital Duplicators, Mailing Machines)
3. Televisions, Multimedia Projectors

This list is continually evolving, and as a result is not all-inclusive.

## **Maintenance, Repairs, Upgrades for the VA Freight Transportation System**

TAC Number: TAC-18-43713

### **ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE**

**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 (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.

## **Maintenance, Repairs, Upgrades for the VA Freight Transportation System**

TAC Number: **TAC-18-43713**

e. The Contractor or Subcontractor must notify the CO 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 CO must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

### **B3. VA INFORMATION CUSTODIAL LANGUAGE**

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

2. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA 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 CO 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.

## **Maintenance, Repairs, Upgrades for the VA Freight Transportation System**

TAC Number: **TAC-18-43713**

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 1600.05, *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 CO 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 CO for response.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require Assessment and Authorization (A&A) or a Memorandum of Understanding-Interconnection Security Agreement (MOU-ISA) for

## **Maintenance, Repairs, Upgrades for the VA Freight Transportation System**

TAC Number: **TAC-18-43713**

system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

### **B4. 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.

### **B5. 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. However, it is the policy of VA to forgo collection of liquidated damages in the event the Contractor provides payment of actual damages in an amount determined to be adequate by the agency.



**Maintenance, Repairs, Upgrades for the VA Freight Transportation System**  
TAC Number: **TAC-18-43713**

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 Breaches Involving Sensitive Personal Information*, 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.

## **Maintenance, Repairs, Upgrades for the VA Freight Transportation System**

TAC Number: **TAC-18-43713**

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.

### **B6. 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 CO 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.]*

b. The Contractor shall provide to the CO and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 2 days 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.

## **Maintenance, Repairs, Upgrades for the VA Freight Transportation System**

TAC Number: **TAC-18-43713**

### **POINTS OF CONTACT**

#### **VA Program Managers:**

Name: Paul Bunker

Address: 810 Vermont Avenue, NW Room 763M  
Washington, DC 20420

Voice: (202) 461-0233

Email: [Paul.Bunker@va.gov](mailto:Paul.Bunker@va.gov)

Name: Daniel Colter

Address: 810 Vermont Avenue, NW Room 763M  
Washington, DC 20420

Voice: (202) 461-5511

Email: [Daniel.Colter@va.gov](mailto:Daniel.Colter@va.gov)