PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS

Records Center and Vault

Warehouse Labor Support Services

Date: February 5, 2018
TAC-18-44838
PWS Version Number: 1.1

Contents

1.0 BACKGROUND

The Department of Veterans Affairs (VA) operates a 400,000 square foot records storage facility in Neosho, Missouri, known as the Records Center and Vault (RCV). The Center stores approximately 1.8 million 25 to 50 lb. boxes of paper and film based records that belong to the various VA agencies and stations located nation-wide. Barcode technology is used to track the warehouse location of the individual boxes. VA stations submit work orders to the RCV to recall records to their facilities, return records to storage upon completion of the review, and to destroy records once agency retention requirements are met. Record retrievals from the Center's 14-foot tall warehouse shelves are performed manually by using a combination of rolling ladders, narrow-aisled carts, hand jacks, conveyors, and scaffolds.

The work order volumes the RCV receives are dynamic and the labor hour requirements to process them vary based on the actual number of Veterans seeking benefits/medical care and the quantities of records becoming eligible for destruction each year. Historically, the RCV has utilized four to seven contractors to provide support for the recall, refile and return shipping duties, and to assist with general warehouse tasks to physically relocate boxes for storage, housekeeping, and destruction purposes.

The senior VA operations supervisor stationed at the Neosho facility (also the VA Program Manager (VA-PM)), is responsible for daily center operations, has oversight of all records management and support services, and ensures adequate labor is available to meet agency needs.

2.0 APPLICABLE DOCUMENTS

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

1. FIPS Pub 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013
2. 10 U.S.C. § 2224, "Defense Information Assurance Program"
3. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
4. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
5. VA Directive 0710, "Personnel Security and Suitability Program," June 4, 2010, http://www.va.gov/vapubs/
6. VA Handbook 0710, Personnel Security and Suitability Security Program, May 2, 2016, http://www.va.gov/vapubs
7. Office of Management and Budget (OMB) Circular A-130, "Managing Federal Information as a Strategic Resource," July 28, 2016
8. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
9. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, 2012
10. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," March 10, 2015

11. VA Handbook 6500.1, “Electronic Media Sanitization,” November 03, 2008
12. VA Handbook 6500.2, “Management of Breaches Involving Sensitive Personal Information (SPI),” July 28, 2016
13. VA Handbook 6500.6, “Contract Security,” March 12, 2010
14. VA Directive 6508, “Implementation of Privacy Threshold Analysis and Privacy Impact Assessment,” October 15, 2014
15. VA Handbook 6508.1, “Procedures for Privacy Threshold Analysis and Privacy Impact Assessment,” July 30, 2015
16. VA Directive 6300, Records and Information Management, February 26, 2009
17. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
18. VA Memorandum “Mandatory Use of PIV Multifactor Authentication to VA Information System” (VAIQ# 7613595), June 30, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
19. VA Memorandum “Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges” (VAIQ# 7613597), June 30, 2015; https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
20. VA Memorandum “Use of Personal Email (VAIQ #7581492)”, April 24, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
21. VA Memorandum “Updated VA Information Security Rules of Behavior (VAIQ #7823189)”, September 15, 2017, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28

3.0 SCOPE OF WORK

Contractor shall process work orders to recall records, refile records, and ship recalled records (via express mail carrier) to VA records owning stations, to relocate groups of boxes to designated areas for storage and destruction purposes, and perform facility leak and safety checks, and general housekeeping duties. These efforts require no communications with VA staff outside of the Neosho RCV location, and no riding lift equipment usage.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance shall be a 12-month base from April 1, 2018, through March 31, 2019, with four 12-month options to extend services.

Hours of Operation: The Contractor’s work schedule is Monday through Friday, from 8:00 AM to 4:30 PM CST. The 30-minute lunch period is 12:00 PM to 12:30 PM, and 15-minute breaks begin at 10:00 AM and 2:30 PM. Adjustments to scheduled start/stop times must be approved by the VA-PM.

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

There are ten (10) Federal holidays set by law (USC Title 5 Section 6103) that VA follows. Under current definitions, four are set by date:

New Year's Day	January 1
Independence Day	July 4
Veterans Day	November 11
Christmas Day	December 25

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

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

Martin Luther King's Birthday	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Thanksgiving	Fourth Thursday in November

4.2 PLACE OF PERFORMANCE

All tasks under this PWS shall be performed at the VA facility located in Neosho, Missouri.

4.3 TRAVEL

No travel specific to the work requirements is anticipated. Contractor employees, however, may be required to travel to the VA Medical Center in Fayetteville, Arkansas, approximately 80 miles from the RCV, for fingerprints and badge requirements. All travel expenses related to this requirement shall be borne by the Contractor.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform time-critical RCV services as detailed below. The work environment is very labor intensive and requires long periods of walking, standing, climbing ladders to access records, and repetitive lifting of 25 to 50-lb. boxes to perform the tasks detailed below.

The Contractor shall perform pre-screening of its employees to certify that Contractor staff are eligible to work in the United States, have a stable work history and a clean background history (not wanted by any law enforcement agency, no felony convictions, no drug, theft, burglary, forgery or arson incidents), and is not a previous RCV contract employee that was either terminated or voluntarily resigned before being terminated for performance or attendance issues. All Contractor staff must be able to read, write, speak and understand the English language. Contractor shall provide the Contracting Officer (CO) and Contracting Officer’s Representative (COR) resumes for new Contractor staff to confirm candidates meet minimum requirements of the PWS.

The Working Team Lead shall possess the following minimum qualifications:

1. High school diploma or GED. Some education above high school is preferred.
2. Experience working in a structured, production-oriented environment.
3. Seven or more years of stable work history gained post high school with at least 3 of those years spent in a supervisory position.
4. Good grammatical, verbal, written communication and coordination skills. Proficiency in Microsoft Office Suite to generate email, reports, training materials, and other documentation.
5. Knowledge of applicable safety regulations and OSHA reporting requirements.
6. Ability to lift 25 to 50 lbs. repetitively, walk and stand long periods of time, and repetitive climbing of 12-foot ladders to perform picking and filing duties.
7. Ability to perform/complete tasks accurately, efficiently and independently.

The Warehouse Support Staff shall possess the following minimum qualifications:

1. High school diploma/GED, or must pass a written skills test with a minimum score of 80% (format of basic skills test to be approved by the VA-PM.) Skills test shall demonstrate candidate can perform basic mathematics/problem solving skills without using a calculator, can place sequences of numbers in correct order, and recognizes differences in spelling of similar names and addresses.
2. Ability to lift 25 to 50 lbs. repetitively, walk long distances, perform repetitive daily climbing of 12' ladders to access records stored on shelves.
3. Minimum 5-year stable work history gained post high school. Two of the five years spent in environments that demonstrate candidate's ability to follow instructions, complete detailed work processes and meet daily processing deadlines.
4. Ability to perform/complete tasks accurately, efficiently and independently.

5.1 PROJECT MANAGEMENT

5.1.1 Project Management Support

The Contractor shall supply a Working Team Lead to provide supervision and training for staff members under this PWS. Working Team Lead shall manage contractor staff to ensure time-frames are met for work completion.

The Contractor's Working Team Lead shall also provide new employee orientation training, safety training, and training on processes and procedures to perform duties for this PWS.

5.1.2 Quality Control

The Contractor shall establish a Quality Control (QC) Plan and implement a program in accordance with the QC plan to ensure accuracy and efficiency of employees performing assigned tasks under this PWS. The program shall be a system for

identifying and correcting deficiencies in the quality of services before the level of performance becomes unacceptable and/or the RCV inspectors point out deficiencies. Revisions to the QC Plan shall be provided to the COR within 24 hours following modification. QC plans developed shall ensure individual employees do not QC their own work efforts.

NOTE: The records stored in the RCV are original hard copies (paper, film, fiche, etc.) with no known backups. Contractor chain of custody must be fully documented on work orders of all actions taken during processing. This includes verifying capture of accurate identifiers and volume count of all boxes/folders/items retrieved (recalled), refiled or shipped, along with the names/dates/times of all staff in contact with the boxes/contents during all processing activities, and capture of the corresponding routing and tracking numbers utilized to ship records to requesting stations.

Deliverable:

A. Quality Control Plan

5.2 REPORTING REQUIREMENTS

The Contractor shall provide the reports outlined below in electronic form in Microsoft Word and Project formats.

5.2.1 Monthly Status Report

The Contractor Monthly Status Report is due to the Contracting Officer's Representative (COR) NLT the 10th day of the month. The report shall include the following consolidated progress of work performed by Contractor staff during the previous month:

1. Summary of monthly performance metrics (count of actions and labor hours by customer) to process recall, refile and shipping work orders.
2. Accidents occurring during the month and remedies to prevent re-occurrence.
3. Results of monthly quality control checks performed by the Contractor.
4. Summary of bottlenecks/quality control issues and corrective action taken to resolve them. The Contractor shall also meet on a daily basis with the COR or designee (unless otherwise informed) to review/discuss previous day's activities and any conflicts or issues arising or anticipated, implementation of new work procedures, address all facility equipment and safety concerns.

5.2.2 Daily Report of Customer Billable Services

The Contractor shall provide COR or designee copies of all employee Daily Time and Man Hour Forms that lists hours worked by customer and category of services performed. The format to capture increments of less than one hour is at the discretion of the VA (tenths, quarter man-hours, etc.).

5.2.3 Accident Report

The Contractor shall provide accident/injury reports within 24 hours of each event. The report shall include witness names to the incident, equipment involved, incident location (include bay/shelving row/shelving unit information if applicable), results of Contractor's investigation, and the corrective action taken to prevent re-occurrence.

5.2.4 Personnel Report

The Contractor shall provide documentation to the COR of new personnel assigned within two (2) business days of starting work. This documentation shall consist of the following:

1. Written certification that new contract employees have received safety training.
2. Written certification that new contract employees are physically fit to perform assigned duties.
3. Signed Certificate of Confidentiality and Non-Disclosure.
4. Signed Contractor Rules of Behavior.
5. VA training certificates (Privacy and Security Awareness Training).

Deliverables:

A. Monthly Status Report
B. Daily Report of Customer Billable Services
C. Accident Report
D. Personnel Report

5.3 RECALLS

The estimated volume of recall work orders for the performance period is 35,000 annually for the VA medical centers (VHA) and 50,000 annually for VA regional offices (RMC).

Emergency recalls arriving during morning hours require picking and shipping by close of the same business day. Emergency recalls arriving in the afternoon require picking and shipping by close of the following business day. Routine recalls received during the current day and before closing time require picking and shipping before close of the following business day. Recall requests arriving during evenings/weekends/federal holidays are processed as though they were received at 8:00 AM the first business day after the evening/weekend/holiday, and the previously stated rules above apply.

RCV will deliver work orders printed on 3-part carbonless paper to the recall/refile sorter station at approximately 8:00 AM, 10:00 AM, 12:00 PM and 2:00 PM each business day.

5.3.1 Processing Recalls

The Contractor shall:

1. Process recall work orders in warehouse areas assigned by the COR to meet processing time-frames outlined in Section 5.3 of this PWS.

2. Post Contract employee room assignments on the outbound mail room bulletin board. If Contractor rotates assignments, do so on the first business day of the month.

3. Notify the COR or designee via email of all instances where either overages or shortages of work required Contractor staff to assist with processing duties in non-assigned areas.

4. Process recalls by warehouse room in ascending row/unit/shelf order, picking all recalls in each row before moving to the next.

5. Mark individual work order forms with the picker's processing information (initials, date, time, type of service performed, the count and description of items pulled, and any folder/file number discrepancies observed). Place the original (white copy) of the work order either on the shelf (for a full box recall) or inside the box (for folder recalls) as a charge out card at the location folders were removed from the box. For VHA recalls, write the warehouse shelf location (bay/row/unit/shelf) and accession and box sequence number the files were removed onto the upper right-hand corner of each folder or envelope removed from the box. Cross out any prior accession and warehouse entries on the front of folders that don't match the current warehouse and accession/box sequence number locators. Secure the remaining two copies of the work order with rubber bands both length-wise and width-wise to the corresponding folder(s). For records in envelopes, staple two corners of both copies of the work order to the envelope to ensure the copy of the work order stay with the records for delivery to the requesting VA station.

6. Deliver and sort processed recall work orders for folders onto the corresponding customer (VHA/RMC) racks for express mail shipping. Deliver to the VA processing table for review all recalls requesting fax or scan services, whole box recalls, and any recall where the file name(s) and number(s) on the work orders were not an exact match to folders removed from a box. VA technicians will re-verify for all folders delivered to the exceptions table that Contractor has captured accurate first/last name identifiers and a full file number to positively identify the records in case they are lost in transit to the customer.

5.3.2 Processing Recalls Where Folders Were Previously Checked Out

Contractor shall code form as a “duplicate request” and capture from the charge out card the date files were previously removed from the box, the first/last name of previous requester, requester’s agency code and city/state location, and number and type of items pulled. If the previous and current requester names on both work orders are the same, use “same requester” for the name, and capture the date/time the previous request was processed.

5.3.3 Processing Recalls Where File Folders Are Not Found

Contractor shall code form as a “no find” and capture the last name and full file number for the first and last file in the box.

5.4 REFILES

The estimated number of refile receipts during the performance period is 25,000 annually. Contractor shall process folder refile work orders within five business days following the date that the requests were initialed/dated/stamped as received by the RCV staff. Processing information and discrepancies shall be documented on the work orders. Deliver processed work order forms and requests unable to be processed as submitted by the customer in collection bins marked for VA review. VA staff will either correct the discrepancies and return the folder refiles to Contractor for processing, or prepare a shipping work order to return the folders to the requesting station.

5.4.1 Processing Re-files of Customer Folders

Contractor shall remove rubber bands/binder clips to return previously recalled items to their original storage container. The corresponding charge-out card shall be pulled and stapled behind the matching refile work order when all files/envelopes previously recalled are returned. Where all previously recalled folder volumes are not returned, the Contractor shall document the corresponding charge out card with the processor’s initials and date/time, the actual count of folder volumes and description of items re-filed, and return the charge out card to the box and mark the refile cover sheet with “Pull Slip in Box”.

5.4.2 Adding New Files to an Existing Box

RCV occasionally receives refile work orders to add new folders to an existing box. Contractor shall perform this service where there is room in the box to add additional files, and there are either files belonging to same Veteran already in the box, or the file range of the refile folder and the box contents match. Where neither of these conditions exist capture the last name and file number of the first and last file on the refile request and folders will be returned to the VHA station unprocessed.

5.5 OUTBOUND MAIL PROCESSING (NON-FREIGHT DELIVERIES)

Contractor shall perform activities to package, ship, and track recalled records and other miscellaneous mail bound for VHA stations. RCV estimates approximately 10,000 packages annually during the period of performance. The Contractor shall perform the duties below:

1. Process outgoing VHA mail to meet time-frames outlined in Section 5.3 above while also combining requests from the same initiator and/or station whenever possible to decrease package count and shipping costs.
2. Maintain current VHA shipping addresses in electronic mail metering equipment.
3. Electronically track total number of outgoing boxes/packages shipped daily.
4. Electronically track via Excel spreadsheet monthly totals for postage and non-freight shipping expense by station ID number.
5. Enter recall processing and shipping results into a standardized electronic template located in the Records Retrieval System (RRS) database.
6. File working copies of processed shipping documents by request submit date. Make new folders as required and transfer files from prior years to inactive storage.
7. Order replenishment shipping supplies furnished free by express mail carriers.
8. Notify designated RCV staff two weeks before depleting office and warehouse supplies needed for shipping purposes (tape, 1-cubic foot corrugated boxes, etc.)

Utilize the express mail service with tracking capabilities designated by the VA-PM to ship all packages containing sensitive information, Personally Identifiable Information (PII) or Protected Health Information (PHI).

Ship records to ensure no packages are in transit during federal holidays or non-business days unless the customer requests emergency or overnight service in writing.

Only ship records to an alternate VA office when the requesting station provides complete contact and mailing information for the alternate in the comments section of the recall work order (recipient’s full name, VA business phone number with area code/complete mailing address).

Deliver processed recalls with notes in the remarks section for scan/fax/search services to the VA review table for processing.

Contractor shall prepare for express mail shipping whole boxes of records recalled from the warehouse and individual files secured in new packaging to authorized requesters as follows:

1. Obtain written approval from the VA-PM/COR or designee before shipping any boxes containing plastic liners or wet/damaged files.
2. Begin package processing after the 10:00 AM deadline for all previous day recalls to be completed and on the racks for shipping. Express mail carrier pickup occurs at approximately 3:00 PM daily.

3. Leave enough room in the packaging to allow opening without damage to internal contents.
4. Replace existing boxes when structural or adhesive weaknesses are observed, there is presence of sensitive information/PII/PHI on the box exterior surface, or box hand holds cannot be secured to prevent visibility/access to records.
5. Include a privacy flyer and verify a copy of the applicable work order(s)/routing slip(s) accompany boxes/packages processed for shipping.
6. Verify outgoing boxes and packages are adequately addressed, sealed, and free of visible, sensitive information before they leave the mail room.
7. Audit individual packages to confirm addresses on recall work orders and package shipping labels match.
8. Run daily shipping manifest/end of day reports from shipping vendor's software and include with packages for express mail carrier pick-up.

5.5.1 Reporting Mail Processing Errors

The Contractor shall advise the COR or designee immediately following discovery of all outgoing mail shipping errors (i.e., shipping files to the wrong VHA station, etc.) to determine whether a reportable privacy incident has occurred. Any Contractor information provided via email to RCV containing sensitive information, PII or PHI must be encrypted.

5.6 WAREHOUSE SUPPORT

5.6.1 Conducting Facility Leak Inspections

The Contractor shall utilize ladders to perform weekly leak inspections in assigned shelving aisles. Leaks found shall be documented in writing on RCV provided forms indicating bay/row/unit location and source of the leak (panning, ceiling, sprinkler head, etc.). Leaks wetting boxes shall immediately be reported by phone to the COR or designee. Completed leak check repair forms are due to the COR or designee by end of the inspection day when leaks are found.

Deliverables:

A. Leak Check Repair Form

5.6.2 Carting, Labeling, Shelving Boxes

The Contractor shall cart, label, shelve, repair, and relocate boxes in accordance with applicable RCV processing procedures. Scenarios requiring these services include repair/relocation of boxes that receive water damage, recall of entire accessions (sets) of boxes by customer, retrieval of accessions of records approved by customer for destruction, repair/re-application of barcode labels that have fallen off of boxes, etc.

5.6.3 General Facility Maintenance

While RCV provides janitorial services, the Contractor shall ensure that facility office space, break room, bathrooms, warehouse aisles, and dock remain in an un-littered condition during each business day. Contractor shall perform general maintenance duties to include organization of supply areas, relocation of furniture to allow cleaning of facility floors, etc. Contract employees utilizing desks are responsible for dusting and maintaining their work space in an organized manner.

The Contractor shall monitor the Government Furnished Equipment (GFE) and facility to ensure they are kept in good repair, reporting all problems via email to the COR or designee. The Contractor shall comply with RCV-established maintenance programs. The Government-provided ladders shall be maintained in shelving row aisles not designated as emergency exits and sit flush with shelving units posts installed at the facility main 10' aisle-way when not in use. All facility equipment (ladders, carts, etc.) shall be stored to prevent compromise to facility egress routes, designated emergency exits, or fire extinguisher access aisles.

5.6.4 Training

New employees shall be trained within 90 days of hire on VA processes required under this task order. The Contractor shall monitor performance and provide remedial training to employees unable to meet processing time-frames. Also the Contractor shall devise and implement a new employee training program to be completed by new hires before they are released to perform critical jobs by themselves without supervision (i.e., performing record shipment mailings, independent processing of recall and refile work orders, etc.) The Contractor shall notify the COR as new hires complete the training program.

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

6.1.1 One-VA Technical Reference Model

N/A. PWS has no IT components.

6.1.2 Federal Identity, Credential, and Access Management (FICAM)

N/A. PWS has no IT components.

6.1.3 Internet Protocol Version 6 (IPV6)

N/A. PWS has no IT components.

6.1.4 Trusted Internet Connection (TIC)

N/A. PWS has no IT components.

6.1.5 Standard Computer Configuration

N/A. PWS has no IT components.

6.1.6 Veteran Focused Integration Process (VIP)

N/A. PWS has no IT components.

6.1.7 Process Asset Library (PAL)

N/A. PWS has no IT components.

6.2 SECURITY AND PRIVACY REQUIREMENTS

It has been determined that protected health information may be disclosed or accessed and a signed Business Associate Agreement (BAA) shall be required. The Contractor shall adhere to the requirements set forth within the BAA, referenced in Section D of the contract, and shall comply with VA Directive 6066.

6.2.1 Position/Task Risk Designation Level(s)

In accordance with VA Handbook 0710, Personnel Security and Suitability Program, 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	☒	☐	☐
5.2	☒	☐	☐
5.3	☒	☐	☐
5.4	☒	☐	☐
5.5	☒	☐	☐
5.6	☒	☐	☐

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

Background Investigation Level for each Contractor individual based upon the tasks the Contractor individual will be working, in accordance with their submitted proposal.

6.2.2 Contractor Personnel Security Requirements

Contractor Responsibilities:

a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
b. 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 PAL template artifact. 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), employee email address for the VA Security and Investigations Center to forward forms to be completed for background investigations, 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).

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.

Performance Objective	Performance Standard	Acceptable Levels of Performance
A. VHA Package Processing Efficiency	Total boxes/packages shipped by the Contractor during a given month is divided by total hours utilized by all Contractor employees to perform shipping actions. Maximum preparation time is 4 minutes per package	99.5% of the time measured on a monthly basis.
B. VHA Package Processing Accuracy	All packages containing Veteran PII/PI deliver successfully to customer.	100% of the time. Each occurrence will be monitored.
C. Recall Processing Efficiency	Total recalls processed by the Contractor is divided by total hours the Contractor expended to perform the task. The maximum acceptable processing time for Veterans Health Administration (VHA) recalls is 5 minutes per request, and Records Management Center (RMC) recalls is 3 minutes per request.	99.5% of the time measured on a monthly basis
D. Recalls Processing Accuracy	Recall orders are accurately filled.	100% of the time. Each occurrence will be monitored.
E. Refiles Processing Efficiency	Total refiles processed by Contractor is divided by total hours the Contractor expended to perform the task. The maximum acceptable processing time is 4 minutes per action.	99.5% of the time measured on a monthly basis.
F. Refiles Processing Accuracy	Refiles are returned to the requested accession and box sequence number.	100% of the time. Each occurrence will be monitored.

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 RCV is located in an underground facility. It contains office areas, a conference room, break room, mail rooms, and restrooms. There is also a two-bay loading dock accessible to two, 18-wheel freight trucks and an enclosed staging area. The only designated smoking area (includes smoking, dipping, chewing, vaping, etc.) resides outside the main cave entrance. A limited amount of employee parking is available inside the cave, with additional spaces located in the outdoors parking lot shared with other Ozark Terminal tenants. Employees will be issued parking permits. Vehicles left inside the cave without proper identification or permission from the senior RCV supervisor to remain after regularly scheduled business hours will be towed at the vehicle owner's expense. Loitering in either parking area is prohibited.

The Government shall provide the RCV facility, including all infrastructure equipment, operating equipment (i.e., ladders, specialized carts), ADP equipment, software and technical support, telecommunications, maintenance and service contracts (i.e., security, pest control, and cleaning services), office equipment, office furniture, and supplies. All work stations (consisting of CPU, monitor, keyboard and mouse) and LAN printers will be provided for Contractor's use where required. The workstations shall only be used as authorized. All procedural guides, reference materials, and program documentation for the project and other Government applications will also be provided on an as-needed basis.

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

6.6 GOVERNMENT FURNISHED PROPERTY

6.6.1 Contractor Return of Government Furnished Equipment (GFE)

Individual contractor staff shall be issued an ID badge (PIV card), parking permit, and general warehouse tools of nominal value such as a box knife, to perform duties under this PWS, herein referred to as GFE. The Contractor shall gather and return GFE (including ID badge/PIV card and parking permit) to the COR or designee when a contract employee resigns, is terminated, laid off, called to active military duty, or takes a medical or unpaid leave of absence for more than four (4) weeks. For permanently departing employees, the Contractor shall complete VA Form 3248 (200), Employee Clearance from Indebtedness, and forward to COR the last day the contract employee works

6.7 SHIPMENT OF HARDWARE OR EQUIPMENT

N/A. The Government will provide all hardware or equipment to perform tasks required of this PWS.

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 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

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

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

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

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

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. Section 508 required the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards setting forth a definition of electronic and information technology and the technical and functional criteria for such technology to comply with Section 508. These standards have been developed and published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

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
- ☐ § 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

N/A. PWS has no IT components.

A3.3. Compatibility with Assistive Technology

N/A. PWS has no IT components.

A3.4. Acceptance and Acceptance Testing

N/A. PWS has no IT components.

A4.0 Physical Security & Safety Requirements:

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

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. 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 (includes dipping, chewing, vaping, etc.) is prohibited in the entire RCV facility, anywhere within the interior cave complex, and must only occur outdoors.
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 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, VA-PM and COR are informed within twenty-four (24) hours of any employee termination.
    g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
    h. Contractor does not require access to classified data.
8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
9. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

A6.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

N/A. PWS HAS NO IT COMPONENTS.

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

VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010

B1. GENERAL

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

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

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.

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.

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

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

1. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: 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, *Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.*

2. 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 11 configured to operate on Windows 7 and future versions, as required.

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

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

5. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program and VA Handbook 6500.5, Incorporating Security and Privacy in System Development Lifecycle.

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

7. The Contractor/Subcontractor agrees to:

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

i. The Systems of Records (SOR); and

ii. The design, development, or operation work that the Contractor/Subcontractor is to perform;

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

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

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

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

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

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

9. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as “Systems”), throughout the life of this contract and any extension, warranty, or maintenance periods.

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

10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical**,** but in no event longer than 2 days.

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

12. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the CO 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 network involving VA information must be in accordance with the TIC Reference Architecture and reviewed and approved by VA prior to implementation. For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP).

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.

c. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires A&A of the Contractor's systems in accordance with VA Handbook 6500.3, *Assessment, Authorization and Continuous Monitoring of VA Information Systems* 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 security 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 CO and the ISO for entry into the VA POA&M management process. The Contractor/Subcontractor must use the VA 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 A&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 A&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 the VA network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems

must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

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

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. 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.

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.

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

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

B8. SECURITY CONTROLS COMPLIANCE TESTING

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) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the Information Security Rules of Behavior, updated version located at https://www.voa.va.gov/DocumentView.aspx?DocumentID=4848, relating to access to VA information and information systems;

2) Successfully complete the VA Privacy and Information Security Awareness and Rules of Behavior course (TMS #10176) and complete this required privacy and information security training annually;

3) Successfully complete VHA Privacy Policy Training if Contractor will have access to PHI;

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 the training and documents are complete.

SCHEDULE FOR DELIVERABLES

Note: Days used in the table below refer to calendar days unless otherwise stated. Deliverables with due dates falling on a weekend or holiday shall be submitted the following Government work day after the weekend or holiday.

Task	Deliverable ID	Deliverable Description
5.1.1	A	**Quality Control Plan** Due five (5) days after contract (DAC) and updated monthly thereafter. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.2.1	A	***Monthly Status Report*** Due the tenth (10) day of each month throughout the period of performance (PoP). Electronic submission to: VA PM, COR, CO Inspection: destination Acceptance: destination
5.2.2	B	**Daily Report of Customer Billable Services** Due no later than (NLT) 10:00 AM local time the next business day following the daily report throughout the PoP. Electronic submission to: VA PM, COR, CO Inspection: destination Acceptance: destination
5.2.3	C	**Accident Report** Due within 24 hours of incident occurrence throughout the PoP. Electronic submission to: VA PM, COR, CO Inspection: destination Acceptance: destination
5.2.4	D	**Personnel Report** Due within two (2) business days of new employee starting work throughout the PoP. Electronic submission to: VA PM, COR, CO Inspection: destination Acceptance: destination
5.6.1	A	**Leak Check Repair Forms** Due NLT end of inspection day when leaks are found. Electronic submission to: VA PM COR, CO Inspection: destination Acceptance: destination
6.2.2	A	**Contractor Staff Roster** Due NLT 3 days following Contract award. Electronic submission to: VA PM COR, CO Inspection: destination Acceptance: destination

POINTS OF CONTACT

VA Program Manager/ COR:
Kim Tuggle
RCV Operations Chief
Records Center and Vault
11693 Lime Kiln Drive
Neosho, MO 64850
417-451-4967
kim.tuggle@va.gov

Contracting Officer:
Lateefah Parker
1701 Director's Blvd, Suite 600
Austin, TX 78774
512-981-4424
lateefah.parker@va.gov

Contract Specialist:
Aaron Waltersdorff
1701 Director's Blvd, Suite 600
Austin, TX 78774
512-981-4469
aaron.waltersdorff@va.gov