Sources Sought Notice

SUBJECT* 614-27-1-031-0005 NEW 'Base + 4' DSS Omnicell IVX Vista Interface Agrmt. (Pharmacy) (VA-27-00002619)

GENERAL INFORMATION

CONTRACTING OFFICE'S ZIP CODE*	37129
SOLICITATION NUMBER*	36C24926Q0351
RESPONSE DATE/TIME/ZONE	08-17-2026 10AM CENTRAL TIME, CHICAGO, USA
ARCHIVE	60 DAYS AFTER THE RESPONSE DATE
RECOVERY ACT FUNDS	N
SET-ASIDE	
PRODUCT SERVICE CODE*	7A20
NAICS CODE*	541519
CONTRACTING OFFICE ADDRESS	Department of Veterans Affairs Network Contracting Office 9 (90C) NCO 9 1639 Medical Center Parkway, Suite 204 Murfreesboro TN 37129
POINT OF CONTACT*	Contract Specialist Daymeion Brantley daymeion.brantley@va.gov 615-225-3616

PLACE OF PERFORMANCE

ADDRESS	VA Memphis Healthcare System Lt. Col. Luke Weathers, Jr. VA Medical Center

	116 North Pauline Street
	Memphis TN
POSTAL CODE	38104
COUNTRY	

ADDITIONAL INFORMATION

AGENCY'S URL	https://www.va.gov/
URL DESCRIPTION	https://www.va.gov/
AGENCY CONTACT'S EMAIL ADDRESS	daymeion.brantley@va.gov
EMAIL DESCRIPTION	daymeion.brantley@va.gov

DESCRIPTION

This is not a request for quotes; the Government is seeking information for market research purposes only. VA Network Contracting Office (NCO) 9 is seeking sources interested and capable of providing the items as described in the attached Product Description.

The North American Industry Classification System (NAICS) is 541519 – Other Computer Related Services

The Service Code (PSC) is 7A20 – Application Development Software (Perpetual License Software)

Responses to this notice shall include company/individual name, size status for the above reference NAICS code, a service capability statement, SAM Entity Unique Identifier (EUI), address, point of contact, and examples of similar facilities to which similar items have been provided.

Contractors must provide information on whether they are certified SDVOSB, VOSB, Hub zone, 8(a), women-owned concern. If standard company brochures will be provided as a response to this Source Sought ensure that additional information tailored to this notice is included.
This is not a solicitation for quotes. If a solicitation is issued, it will be announced on the Contract Opportunities website https: respond to that solicitation announcement separately from the response to this announcement.

Contractors must be registered in System for Award Management (SAM), see internet site: https://www.sam.gov for information about registration.

Identify any other companies owned (wholly or in-part) by the owners of this business who provide goods or services that are registered under the same or a related NAICS code with the Center for Veterans Enterprise (CVE); Provide the certification type (SDVOSB/VOSB), Federal Identification Number, and state of incorporation for each.

Do you plan on responding to a solicitation for this requirement with a Joint Venture utilizing multiple owned companies as majority or non-majority owner?

If you are in GSA, please provide schedule and contract number.
Responses to this notice must be submitted via email to daymeion.brantley@va.gov. No telephone inquiries will be accepted.

DISCLAIMER This Sources Sought is issued solely for information and planning purposes only and does not constitute a solicitation. All information received in response to this Sources Sought that is marked as proprietary will be handled accordingly. Responses to this notice are not offers and cannot be accepted by the Government to form a binding contract. Responders are solely responsible for all expenses associated with responding to this Sources Sought.

Veterans Affairs, NCO-9, is seeking information for vendors interested and capable of providing the service below:

Omnicell IVX® Compound Sterile Products Processing, Verification, and Archiving System – Document Storage Solutions, Inc.
Pharmacy Service

STATEMENT OF WORK PART A – GENERAL INFORMATION

A.1 INTRODUCTION
This document is intended to initiate requirements on current and future technology interface requirements at the Memphis VA Medical Center for pharmacy systems.

A.2 BACKGROUND
Pharmacy technology needs are continuously evolving, and technology is continuously advancing placing information interface strains on aged VA VISTA OIT infrastructure. As such many newer technologies require enterprise solutions to data sharing in security protected operationally functional information streams which can be handled by both the newer technology and the aged VA OIT infrastructure.

A.3 SCOPE OF WORK
Document Storage Solutions, Incorporated (DSS) is an enterprise solution specialty company specific to VA hardware and software solutions. They publish with the GSA a full suite of solutions individualized by supported non-VA venders to allow non-VA vender technology communications with VA systems. They are unique in the marketplace and technology, or technology upgrades require their interface applications for update and retrieve patient data that is held in an M (MUMPS) data repository or SQL database systems.

STATEMENT OF WORK PART B – WORK REQUIREMENTS

Describe the tasks to be accomplished. Describe the work in detail. Divide the work into tasks. Describe tasks as what is to be accomplished. Identify and describe the key elements of each task.

TASK	COMPLETION CRITERIA
Maintain a network interface for the Omnicell IVX server in accordance with established Department of Veterans Affairs guidelines for servers with HIPAA and patient specific information.	The interface responds appropriately to PING command and communicates with all current and future associated devices.
Provide/configure connectivity to the Omnicell IVX server. Install and configure DSSRX-Omnicell-IVX-P software to allow full functionality of the Omnicell IVX and VA information systems' communications.	All Omnicell IVX devices, both local and remote, communicate with the Omnicell IVX server
DSSRX-Omnicell-IVX-M software maintenance and support to allow full functionality of the DSSRX-Omnicell-IVX-P and VA information systems' Communications Omnicell IVX devices are assigned appropriate IP addresses. IRM will generate IP addresses. IRM will compare the optimal specifications to the existing systems and equipment and determine the need to change any local settings (such as a VLAN).	DSS, inc. maintains the DSSRX-Omnicell-IVX-P software interface between the Omnicell IVX and VA systems to full functionality of secure data sharing. Each Omnicell IVX device that connects to and communicates with Omnicell IVX server has an IP address and DSS personnel use the assigned IP address to test and maintain the communication interface.

STATEMENT OF WORK PART C – SUPPORTING INFORMATION

C.1. Place of Performance [all addresses]

C1.1. Pharmacy Service – main servers and remote workstations

C.2. Period of Performance – [10/01/2026 through 09/30/2031 with 4 12-month options beginning 10/1/2027.] Routine maintenance, routine and emergency service, non-routine service to include software updates and necessary upgrades for the duration of the contract including base and 4 option years.

C2.1. Government Furnished Materials and Services

C2.1.1. Memphis VAMC will furnish an intact, operational data network and server host site sufficient for effective day-to-day operation of the DSSRX-Omnicell-IVX-P software.

C2.2. Qualifications of Key Personnel

C2.2.1. DSS Inc. will ensure that personnel furnished for DSSRX-Omnicell-IVX-P software configuration, maintenance and support have sufficient experience and knowledge to properly provide all services.

C2.3. Security Requirements

C2.3.1. DSS, inc. Omnicell IVX software communication solution [DSSRX-Omnicell-IVX-P] over VA network connections is considered secure as measured against Department of Veterans Affairs National, regional and local guidelines.

C2.3.2. Part of the DSSRX-Omnicell-IVX-P maintenance contract with DSS, inc. will allow and require remote access to the VA System by DSS. Inc. technical personnel. DSS, inc. will set up an account with the Department of Veterans Affairs that permits communication with the local VA System(s) via Virtual Private Network (VPN). Under certain catastrophic circumstances, communication via modem MAY be allowed (providing all permissions to use the modem are granted through the facility ISO).

C2.3.3. Information Systems Security

2.3.3.1. Access to DSS, inc. and Omnicell IVX software and hardware operation is protected by the same safeguards as is standard on all Department of Veteran's Affairs workstations and servers and is compliant with national guidelines.

2.3.3.2. Antiviral software, firewall software and any other software necessary to secure uninterrupted operation and protect sensitive VA data will be applied to the DSS, Inc. and Omnicell IVX servers as is standard for all Department of Veteran's Affairs workstations and servers and compliant with national guidelines.

2.3.3.3. DSS, inc. will have and maintain a Business Access Agreement with the Department of Veterans Affairs and comply with requirements detailed below in C2.3.3.4

2.3.3.4. “VAAR- 852.273-75 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (Interim - October 2008)

2.3.3.5. The contractor and their personnel shall be subject to the same Federal laws, regulations, standards and VA policies as VA personnel, regarding information and information system security. These include but are not limited to Federal Information Security Management Act (FISMA), Appendix III of 0MB Circular A-130, and guidance and standards, available from the Department of Commerce’s National Institute of Standards and Technology (NIST). This also includes the use of common security configurations available from NIST’s Web site at: http://checklists.nist.gov

2.3.3.6. To ensure that appropriate security controls are in place, contractors must follow the procedures set forth in "VA Information and Information System Security/Privacy Requirements for IT Contracts" located at the following Web site: http://www.iprm.oit.va.gov\

2.3.3.7. These provisions shall apply to all contracts in which VA sensitive information is stored, generated, transmitted, or exchanged by VA, a contractor, subcontractor or a third-party, or on behalf of any of these entities regardless of format or whether it resides on a VA system or contractor/subcontractor's electronic information system(s) operating for or on the VA's behalf.

2.3.3.8. Clauses 3.4.4.5 and 3.4.4.6 shall apply to current and future contracts and acquisition vehicles including, but not limited to, task orders, letter contracts, purchase orders, and modifications. Contracts do not include grants and cooperative agreements covered by 31 U.S.C. §6301 et seq.

2.3.3.9. Certification of Compliance.

I certify that all requirements applicable to this contract follow the stated clause VAAR Clause 852.273-75.

2.3.3.10.

_____

Authorized Company Representative Signature

2.3.3.11. Contractor's Statement of Release - In consideration of the modification agreed to herein as complete equitable adjustment, the Contractor hereby releases the Government from all liability under this contract for further equitable adjustments attributable to this modification.

2.3.3.12. Memphis VAMC will provide a secure or observable area for operating each device of the Omnicell system.

Schedule of Costs

Line Item	Description	Quantity	Unit of Measure	Unit Price	Total Price
0001	**Base Year: 10/1/2026 – 9/30/2027. DSS Omnicell IVX VISTA Interface software subscription maintenance and support M-F, 8-8 EST, includes bug fixes, minor release upgrades, telephone support for a period of one year**	**1**	**EA**		
1001	**Option Year One: 10/1/2027 – 9/30/2028. DSS Omnicell IVX VISTA Interface software subscription maintenance and support M-F, 8-8 EST, includes bug fixes, minor release upgrades, telephone support for a period of one year**	**1**	**EA**		
2001	**Option Year Two: 10/1/2028 – 9/30/2029. DSS Omnicell IVX VISTA Interface software subscription maintenance and support M-F, 8-8 EST, includes bug fixes, minor release**	**1**	**EA**		

	upgrades, telephone support for a period of one year				
3001	**Option Year Three: 10/1/2029 – 9/30/2030. DSS Omnicell IVX VISTA Interface software subscription maintenance and support M-F, 8-8 EST, includes bug fixes, minor release upgrades, telephone support for a period of one year**	**1**	**EA**		
4001	**Option Year Four: 10/1/2030 – 9/30/2031. DSS Omnicell IVX VISTA Interface software subscription maintenance and support M-F, 8-8 EST, includes bug fixes, minor release upgrades, telephone support for a period of one year**	**1**	**EA**		
Total Price					

APPENDIX B

VA ACQUISITION REGULATION SOLICITATION PROVISION AND CONTRACT CLAUSE
NOTE: This clause will undergo official rule making by the Office of Acquisitions and Logistics. The language below will be submitted for public review through the Federal Register. The final wording of the clause may be changed from what is outlined below based on public review and comment. Once approved, the final language in the clause can be obtained from the Office of Acquisitions and Logistics Programs and Policy.

1. SUBPART 839.2 – INFORMATION AND INFORMATION TECHNOLOGY SECURITY REQUIREMENTS 839.201 Contract clause for Information and Information Technology Security:

a. Due to the threat of data breach, compromise or loss of information that resides on either VA-owned or contractor-owned systems, and to comply with Federal laws and regulations, VA has developed an Information and Information Technology Security clause to be used when VA sensitive information is accessed, used, stored, generated, transmitted, or exchanged by and between VA and a contractor, subcontractor or a third party in any format (e.g., paper, microfiche, electronic or magnetic portable media).

b. In solicitations and contracts where VA Sensitive Information or Information Technology will be accessed or utilized, the CO shall insert the clause found at 852.273-75, Security Requirements for Unclassified Information Technology Resources.

2. 852.273-75 - SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (INTERIM- OCTOBER 2008)
As prescribed in 839.201, insert the following clause:
The contractor, their personnel, and their subcontractors shall be subject to the Federal laws, regulations, standards, and VA Directives and Handbooks regarding information and information system security as delineated in this contract.

The C&A requirements do not apply, and the Security Accreditation Package is not required.

(END OF CLAUSE)

APPENDIX C — VA INFORMATION AND INFORMATION SYSTEM SECURITY AND PRIVACY LANGUAGE FOR INCLUSION IN CONTRACTS, AS APPROPRIATE

NOTE: Any sections (1-14) which DO NOT apply should not be included in the Statement of Work (SOW), Performance Work Statement (PWS), Product Description (PD) or contract.

1. **GENERAL**. This entire section applies to all acquisitions requiring any Information Security and Privacy language. Contractors, contractor personnel, subcontractors and subcontractor personnel will be subject to the same federal laws, regulations, standards, VA directives and handbooks, as VA personnel regarding information and information system security and privacy.

2. **VA INFORMATION CUSTODIAL LANGUAGE**. This entire section applies to all acquisitions requiring any Information Security and Privacy language.

a. The Government shall receive unlimited rights to data/intellectual property first produced and delivered in the performance of this contract or order (hereinafter "contract") unless expressly stated otherwise in this contract. This includes all rights to source code and all documentation created in support thereof. The primary clause used to define Government and Contractor data rights is FAR 52.227-14 Rights in Data – General. The primary clause used to define computer software license (not data/intellectual property first produced under this contractor or order) is FAR 52.227-19, Commercial Computer Software License.

b. Information made available to the contractor by VA for the performance or administration of this contract will be used only for the purposes specified in the service agreement, SOW, PWS, PD, and/or contract. The contractor shall not use VA information in any other manner without prior written approval from a VA Contracting Officer (CO). The primary clause used to define Government and Contractor data rights is FAR 52.227-14 Rights in Data – General.

c. VA information will not be co-mingled with any other data on the contractor's information systems or media storage systems. The contractor shall ensure compliance with Federal and VA requirements related to data protection, data encryption, physical data segregation, logical data segregation, classification requirements and media sanitization.

d. VA reserves the right to conduct scheduled or unscheduled audits, assessments, or investigations of contractor Information Technology (IT) resources to ensure information security is compliant with Federal and VA requirements. The contractor shall provide all necessary access to records (including electronic and documentary materials related to the contracts and subcontracts) and support (including access to contractor and subcontractor staff associated with the contract) to VA, VA's Office Inspector General (OIG), and/or Government Accountability Office (GAO) staff during periodic control assessments, audits, or investigations.

e. The contractor may only use VA information within the terms of the contract and applicable Federal law, regulations, and VA policies. If new Federal information security laws, regulations or VA policies become applicable after execution of the contract, the parties agree to negotiate contract modification and adjustment necessary to implement the new laws, regulations, and/or policies.

f. The contractor shall not make copies of VA information except as specifically authorized and necessary to fulfil the terms of the contract. If copies are made for restoration purposes, after the restoration is complete, the copies shall be destroyed in accordance with VA Directive 6500, VA Cybersecurity Program and VA Information Security Knowledge Service.

g. If a Veterans Health Administration (VHA) contract is terminated for default or cause with a business associate, the related local Business Associate Agreement (BAA) shall also be terminated and actions taken in accordance with VHA Directive 1605.05, Business Associate Agreements. If there is an executed national BAA associated with the contract, VA will determine what actions are appropriate and notify the contactor.

h. The contractor shall store and transmit VA sensitive information in an encrypted form, using VA-approved encryption tools which are, at a minimum, Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules (or its successor) validated and in conformance to VA Information Security Knowledge Service requirements. The contractor shall transmit VA sensitive information using VA approved Transport Layer Security (TLS) configured with FIPS based cipher suites in conformance with National Institute of Standards and Technology (NIST) 800-52, Guidelines for the Selection, Configuration and Use of Transport Layer Security (TLS) Implementations.

i. The contractor's firewall and web services security controls, as applicable, shall meet or exceed VA's minimum requirements.

j. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor may use and disclose VA information only in two situations: (i) in response to a qualifying order of a court of competent jurisdiction after notification to VA CO (ii) with written approval from the VA CO. The contractor shall refer to all requests for demands for production of or inquiries about VA information and information systems to the VA CO for response.

k. Notwithstanding the provision above, the contractor 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 medical records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse or infection with Human Immunodeficiency Virus (HIV). If the contractor is in receipt of a court order or other requests for the above-mentioned information, the contractor shall immediately refer to such court order or other requests to the VA CO for response.

l. Information made available to the contractor by VA for the performance or administration of this contract or information developed by the contractor in performance or administration of the contract will be protected and secured in accordance with VA Directive 6500 and Identity and Access Management (IAM) Security processes specified in the VA Information Security Knowledge Service.

m. Any data destruction done on behalf of VA by a contractor shall be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management, VA Handbook 6300.1, Records Management Procedures, and applicable VA Records Control Schedules.

n. The contractor shall provide its plan for destruction of all VA data in its possession according to VA Directive 6500 and NIST 800-88, Guidelines for Media Sanitization prior to termination or completion of this contract. If directed by the COR/CO, the contractor shall return all Federal Records to VA for disposition.

o. Any media, such as paper, magnetic tape, magnetic disks, solid state devices or optical discs that are used to store, process, or access VA information that cannot be destroyed shall be returned to VA. The contractor shall hold the appropriate material until otherwise directed by the Contracting Officer's Representative (COR) or CO. Items shall be returned securely via VA-approved methods. VA sensitive information must be transmitted utilizing VA-approved encryption tools which are validated under FIPS 140-2 (or its successor) and NIST 800-52. If mailed, the contractor shall send via a trackable method (USPS, UPS, FedEx, etc.) and immediately provide the COR/CO with the tracking information. Self-

certification by the contractor that the data destruction requirements above have been met shall be sent to the COR/CO within 30 business days of termination of the contract.

p. All electronic storage media (hard drives, optical disks, CDs, back-up tapes, etc.) used to store, process or access VA information will not be returned to the contractor at the end of lease, loan, or trade-in. Exceptions to this paragraph will only be granted with the written approval of VA CO.

3. **ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS.** This section applies when any person requires access to information made available to the contractor by VA for the performance or administration of this contract or information developed by the contractor in performance or administration of the contract.

   a. A contractor/subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees and subcontractors only to the extent necessary to perform the services specified in the solicitation or contract. This includes indirect entities, both affiliate of contractor/subcontractor and agent of contractor/subcontractor.

   b. Contractors and subcontractors shall sign the VA Information Security Rule of Behavior (ROB) before access is provided to VA information and information systems (see Section 4, Training, below). The ROB contains the minimum user compliance requirements and does not supersede any policies of VA facilities or other agency components which provide higher levels of protection to VA's information or information systems. Users who require privileged access shall complete the VA elevated privilege access request processes before privileged access is granted.

   c. All contractors and subcontractors working with VA information are subject to the same security investigative and clearance 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 shall be in accordance with VA Directive and Handbook 0710, Personnel Suitability and Security Program. The Office of Human Resources and Administration/Operations, Security and Preparedness (HRA/OSP) is responsible for these policies and procedures. Contract personnel who require access to classified information or information systems shall have an appropriate security clearance. Verification of Security Clearance shall be processed through the Special Security Officer located in HRA/OSP. Contractors shall conform to all requirements stated in the National Industrial Security Program Operating Manual (NISPOM).

   d. All contractors and subcontractors shall comply with conditions specified in VAAR 852.204-71(d); Contractor operations required to be in United States. All contractors and subcontractors working with VA information must be permanently located within a jurisdiction subject to the law of the United States or its Territories to the maximum extent feasible. If services are proposed to be performed abroad the contractor must state where all non-U.S. services are provided. The contractor shall deliver to VA a detailed plan specifically addressing communications, personnel control, data protection and potential legal issues. The plan shall be approved by the COR/CO in writing prior to access being granted.

   e. The contractor shall notify the COR/CO in writing immediately (no later than 24 hours) after personnel separation or occurrence of other causes. Causes may include the following:

      (1) Contractor/subcontractor personnel no longer have a need for access to VA information or VA information systems.

(2) Contractor/subcontractor personnel are terminated, suspended, or otherwise have their work on a VA project discontinued for any reason.

(3) Contractors believe their own personnel or subcontractor personnel may pose a threat to their company's working environment or to any company-owned property. This includes contractor-owned assets, buildings, confidential data, customers, employees, networks, systems, trade secrets and/or VA data.

(4) Any previously undisclosed changes to contractor/subcontractor background history are brought to light, including but not limited to changes to background investigation or employee record.

(5) Contractor/subcontractor personnel have their authorization to work in the United States revoked.

(6) Agreement by which contractor provides products and services to VA has either been fulfilled or terminated, such that VA can cut off electronic and/or physical access for contractor personnel.

f. In such cases of contract fulfillment, termination, or other causes; the contractor shall take the necessary measures to immediately revoke access to VA network, property, information, and information systems (logical and physical) by contractor/subcontractor personnel. These measures include (but are not limited to): removing and then securing Personal Identity Verification (PIV) badges and PIV – Interoperable (PIV-I) access badges, VA-issued photo badges, credentials for VA facilities and devices, VA-issued laptops, and authentication tokens. Contractors shall notify the appropriate VA COR/CO immediately to initiate access removal.

g. Contractors/subcontractors who no longer require VA access will return VA-issued property to VA. This property includes (but is not limited to) documents, electronic equipment, keys, and parking passes. PIV and PIV-I access badges shall be returned to the nearest VA PIV Badge Issuance Office. Once they have had access to VA information, information systems, networks and VA property in their possessions removed, contractors shall notify the appropriate VA COR/CO.

4. TRAINING. This entire section applies to all acquisitions which include section 3.

a. All contractors and subcontractors requiring access to VA information and VA information systems shall successfully complete the following before being granted access to VA information and its systems:

(1) VA Privacy and Information Security Awareness and Rules of Behavior course (Talent Management System (TMS) 10176) initially and annually thereafter.

(2) Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the Organizational Rules of Behavior, relating to access to VA information and information systems initially and annually thereafter; and

(3) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system or information access [to be defined by the VA program official and provided to the VA CO for inclusion in the solicitation document – i.e., any role-based information security training].

b. The contractor shall provide the COR/CO with a copy of the training certificates and certification of signing the Organizational Rules of Behavior for each applicable employee within five days of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training 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 required training is complete.

5. **SECURITY INCIDENT INVESTIGATION.** This entire section applies to all acquisitions requiring any Information Security and Privacy language.

a. The contractor, subcontractor, their employees, or business associates shall immediately (within one hour) report suspected security / privacy incidents to the VA OIT's Enterprise Service Desk (ESD) by calling (855) 673-4357 (TTY: 711). The ESD is OIT's 24/7/365 single point of contact for IT-related issues. After reporting to the ESD, the contractor, subcontractor, their employees, or business associates shall, within one hour, provide the COR/CO with the incident number received from the ESD.

b. To the extent known by the contractor/subcontractor, the contractor/ subcontractor's notice to VA shall identify the information involved and the circumstances surrounding the incident, including the following:

(1) The date and time (or approximation of) the Security Incident occurred.

(2) The names of individuals involved (when applicable).

(3) The physical and logical (if applicable) location of the incident.

(4) Why did the Security Incident take place (i.e., catalyst for the failure).

(5) The amount of data belonging to VA was believed to have been compromised.

(6) The remediation measures the contractor is taking to ensure no future incidents of a similar nature.

c. After the contractor has provided the initial detailed incident summary to VA, they will continue to provide written updates on any new and relevant circumstances or facts they discover. The contractor, subcontractor, and their employes shall fully cooperate with VA or third-party entity performing an independent risk analysis on behalf of VA. Failure to cooperate may be deemed a material breach and grounds for contract termination.

d. VA IT contractors shall follow VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program, and VA Information Security Knowledge Service guidance for implementing an Incident Response Plan or integrating with an existing VA implementation.

e. 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 the VA Office of 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 violations 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.

f. The contractor shall comply with VA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information, which establishes the breach management policies and assigns responsibilities for the oversight, management and reporting procedures associated with managing of breaches.

g. With respect to unsecured Protected Health Information (PHI), the contractor is deemed to have discovered a data breach when the contractor knew or should have known of breach of such information. When a business associate is part of VHA contract, notification to the covered entity (VHA) shall be made in accordance with the executed BAA.

h. If the contractor or any of its agents fails to protect VA sensitive personal information or otherwise engages in conduct which results in a data breach involving any VA sensitive personal information the contractor/subcontractor processes or maintains under the contract; the contractor shall pay liquidated damages to the VA as set forth in clause 852.211-76, Liquidated Damages—Reimbursement for Data Breach Costs.

6. **INFORMATION SYSTEM DESIGN AND DEVELOPMENT.** This entire section applies to information systems, systems, major applications, minor applications, enclaves, and platform information technologies (to include the subcomponents of each) designed or developed for or on behalf of VA by any non-VA entity.

a. Information systems designed or developed on behalf of VA at non-VA facilities shall comply with all applicable Federal law, regulations, and VA policies. This includes standards for the protection of electronic Protected Health Information (PHI), outlined in 45 C.F.R. Part 164, Subpart C and information and system security categorization level designations in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems and FIPS 200, Minimum Security Requirements for Federal Information Systems. Baseline security controls shall be implemented commensurate with the FIPS 199 system security categorization (reference VA Handbook 6500 and VA Trusted Internet Connections (TIC) Architecture).

b. Contracted new developments require creation, testing, evaluation, and authorization in compliance with VA Assessment and Authorization (A&A) processes in VA Handbook 6500 and VA Information Security Knowledge Service to obtain Authority to Operate (ATO). VA Directive 6517, Risk Management Framework for Cloud Computing Services, provides security and privacy requirements for cloud environments.

c. VA IT contractors, subcontractors and third-party service providers shall address and/or integrate applicable VA Handbook 6500, VA Handbook 6517, Risk Management Framework for Cloud Computing Services and Information Security Knowledge Service specifications in delivered IT systems/solutions, products and/or services. If systems/solutions, products and/or services do not directly match VA security requirements, the contractor shall work though the COR/CO to identify the VA organization responsible for governance or resolution. Contractors shall comply with FAR 39.1, specifically the prohibitions referenced.

d. The contractor (including producers and resellers) shall comply with Office of Management and Budget (OMB) M-22-18 and M-23-16 when using third-party software on VA information systems or otherwise affecting the VA information. This includes new software purchases and software renewals for software developed or modified by major version change after the issuance date of M-22-18 (September 14, 2022). The term “software”

includes firmware, operating systems, applications and application services (e.g., cloud-based software), as well as products containing software. The contractor shall provide a self-attestation that secure software development practices are utilized as outlined by Executive Order (EO)14028 and NIST Guidance. A third-party assessment provided by either a certified Federal Risk and Authorization Management Program (FedRAMP) Third Party Assessor Organization (3PAO) or one approved by the agency will be acceptable in lieu of a software producer's self-attestation.

e. The contractor shall ensure all delivered applications, systems and information systems are compliant with Homeland Security Presidential Directive (HSPD) 12 and VA Identity and Access management (IAM) enterprise identity management requirements as set forth in OMB M-19-17, M-05-24, FIPS 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors (or its successor), M-21-31 and supporting NIST guidance. This applies to Commercial Off-The-Shelf (COTS) product(s) that the contractor did not develop, all software configurations and all customizations.

f. The contractor shall ensure all contractors delivered applications and systems provide user authentication services compliant with VA Handbook 6500, VA Information Security Knowledge Service, IAM enterprise requirements and NIST 800-63, Digital Identity Guidelines, for direct, assertion-based authentication and/or trust-based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of PIV and/or Common Access Card (CAC), as determined by the business need and compliance with VA Information Security Knowledge Service specifications.

g. The contractor shall use VA authorized technical security baseline configurations and certify to the COR that applications are fully functional and operate correctly as intended on systems in compliance with VA baselines prior to acceptance or connection into an authorized VA computing environment. If the Defense Information Systems Agency (DISA) has created a Security Technical Implementation Guide (STIG) for the technology, the contractor may configure to comply with that STIG. If VA determines a new or updated VA configuration baseline needs to be created, the contractor shall provide required technical support to develop the configuration settings. FAR 39.1 requires the population of operating systems and applications includes all listed on the NIST National Checklist Program Checklist Repository.

h. The standard installation, operation, maintenance, updating and patching of software shall not alter the configuration settings from VA approved baseline configuration. Software developed for VA must be compatible with VA enterprise installer services and install to the default “program files” directory with silently install and uninstall. The contractor shall perform testing of all updates and patching prior to implementation on VA systems.

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

j. The contractor-delivered solutions shall reside on VA approved operating systems. Exceptions to this will only be granted with the written approval of the COR/CO.

k. The contractor shall design, develop, and implement security and privacy controls in accordance with the provisions of VA security system development life cycle outlined in NIST 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, VA Directive and Handbook 6500, and VA Handbook 6517.

l. The Contractor shall comply with the Privacy Act of1974 (the Act), FAR 52.224-2 Privacy Act, and VA rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish a VA function.

m. The contractor shall ensure the security of all procured or developed information systems, systems, major applications, minor applications, enclaves and platform information technologies, including their subcomponents (hereinafter referred to as "Information Systems") throughout the life of this contract and any extension, warranty, or maintenance periods. This includes security configurations, workarounds, patches, hotfixes, upgrades, replacements and any physical components which may be necessary to remediate all security vulnerabilities published or known to the contractor anywhere in the information systems (including systems, operating systems, products, hardware, software, applications and firmware). The contractor shall ensure security fixes do not negatively impact the Information Systems.

n. When the contractor is responsible for operations or maintenance of the systems, the contractor shall apply the security fixes within the timeframe specified by the associated controls on the VA Information Security Knowledge Service. When security fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the contractor shall provide written notice to the VA COR/CO that the patch has been validated as not affecting the Systems within 10 business days.

7. **INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE OR USE.** This entire section applies to information systems, systems, major applications, minor applications, enclaves, and platform information technologies (cloud and non-cloud) hosted, operated, maintained, or used on behalf of VA at non-VA facilities.

a. The contractor shall comply with all Federal laws, regulations, and VA policies for Information systems (cloud and non-cloud) that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities. Security controls for collecting, processing, transmitting, and storing of VA sensitive information, must be in place. The controls will be tested by VA or a VA sanctioned 3PAO and approved by VA prior to hosting, operation, maintenance or use of the information system or systems by or on behalf of VA. This includes conducting compliance risk assessments, security architecture analysis, routine vulnerability scanning, system patching, changing management procedures and the completion of an acceptable contingency plan for each system. The contractor's security control procedures shall be the same as procedures used to secure VA-operated information systems.

b. Outsourcing (contractor facility, equipment, or staff) of systems or network operations, telecommunications services or other managed services require Assessment and Authorization (A&A) of the contractor's systems in accordance with VA Handbook 6500 as specified in VA Information Security Knowledge Service. Major changes to the A&A package may require reviewing and updating all the documentation associated with the change. The contractor's cloud computing systems shall comply with FedRAMP and VA Directive 6517 requirements.

c. The contractor shall return all electronic storage media (hard drives, optical disks, CDs, back-up tapes, etc.) to non-VA leased or non-VA owned IT equipment used to store, process, or access VA information to VA in accordance with A&A package requirements. This applies when the contract is terminated or completed and prior to disposal of media. The contractor shall provide its plan for destruction of all VA data in its possession according to VA Information Security Knowledge Service requirements and NIST 800-88. The contractor shall send a self-certification that the data destruction requirements above have been met to the COR/CO within 30 business days of termination of the contract.

d. All external internet connections to VA network involving VA information must be in accordance with VA Trusted Internet Connection (TIC) Reference Architecture and VA Directive and Handbook 6513, Secure External Connections and reviewed and approved by VA prior to implementation. Government-owned contractor-operated systems, third party or business partner networks require a Memorandum of Understanding (MOU) and Interconnection Security Agreements (ISA).

e. Contractor procedures shall be subject to periodic, announced, or unannounced assessments by VA officials, the OIG or a 3PAO. The physical security aspects associated with contractor activities are also subject to such assessments. The contractor shall report, in writing, any deficiencies noted during the above assessment to the VA COR/CO. The contractor shall use VA's defined processes to document planned remedial actions that address identified deficiencies in information security policies, procedures, and practices. The contractor shall correct security deficiencies within the timeframes specified in the VA Information Security Knowledge Service.

f. All major information system changes which occur in the production environment shall be reviewed by the VA to determine the impact on privacy and security of the system. Based on the review results, updates to the Authority to Operate (ATO) documentation and parameters may be required to remain in compliance with VA Handbook 6500 and VA Information Security Knowledge Service requirements.

g. The contractor shall conduct an annual privacy and security self-assessment on all information systems and outsourced services as required. Copies of the assessment shall be provided to the COR/CO. The VA/Government reserves the right to conduct assessments using government personnel or a third party if deemed necessary. The contractor shall correct or mitigate any weaknesses discovered during the assessment.

h. VA prohibits the installation and use of personally owned or contractor-owned equipment or software on VA information systems. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW, PWS, PD or contract. All security controls required for government furnished equipment must be utilized in VA approved Other Equipment (OE). Configuration changes to the contractor OE must be funded by the owner of the equipment. All remote systems must use VA-approved antivirus software and a personal (host-based or enclave based) firewall with a VA-approved configuration. The contractor shall ensure software on OE is kept current with all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-virus software and the firewall on the non-VA owned OE. Approved contractor OE will be subject to technical inspection at any time.

i. The contractor shall notify the COR/CO within one hour of disclosure or successful exploits of any vulnerability which can compromise the confidentiality, integrity, or availability of the information systems. The system or effected component(s) needs(s) to be isolated from the network. A forensic analysis needs to be conducted jointly with VA. Such issues will be remediated as quickly as practicable, but in no event longer than the timeframe specified by VA Information Security Knowledge Service. If sensitive personal information is compromised reference VA Handbook 6500.2 and Section 5, Security Incident Investigation.

j. For cases wherein the contractor discovers material defects or vulnerabilities impacting products and services they provide to VA, the contractor shall develop and implement policies and procedures for disclosure to VA, as well as remediation. The contractor shall, within 30 business days of discovery, document a summary of these vulnerabilities or defects. The documentation will include a description of the potential impact of each vulnerability and material defect, compensating security controls, mitigations, recommended corrective actions, root cause analysis

and/or workarounds (i.e., monitoring). Should there exist any backdoors in the products or services they provide to VA (referring to methods for bypassing computer authentication), the contractor shall provide the VA CO/CO written assurance they have permanently remediated these backdoors.

k. All other vulnerabilities, including those discovered through routine scans or other assessments, will be remediated based on risk, in accordance with the remediation timelines specified by the VA Information Security Knowledge Service and/or the applicable timeframe mandated by Cybersecurity & Infrastructure Security Agency (CISA) Binding Operational Directive (BOD) 22-01 and BOD 19-02 for Internet-accessible systems. Exceptions to this paragraph will only be granted with the approval of the COR/CO.

8. SECURITY AND PRIVACY CONTROLS COMPLIANCE TESTING, ASSESSMENT AND AUDITING. This entire section applies whenever section 6 or 7 is included.

a. Should VA request it, the contractor shall provide a copy of their (corporation's, sole proprietorship's, partnership's, limited liability company (LLC), or other business structure entity's) policies, procedures, evidence and independent report summaries related to specified cybersecurity frameworks (International Organization for Standardization (ISO), NIST Cybersecurity Framework (CSF), etc.). VA or its third-party/partner designee (if applicable) are further entitled to perform their own audits and security/penetration tests of the contractor's IT or systems and controls, to ascertain whether the contractor is complying with the information security, network or system requirements mandated in the agreement between VA and the contractor.

b. Any audits or tests of the contractor or third-party designees/partner VA elects to carry out will commence within 30 business days of VA notification. Such audits, tests and assessments may include the following: (a): security/penetration tests which both sides agree will not unduly impact contractor operations; (b): interviews with pertinent stakeholders and practitioners; (c): document review; and (d): technical inspections of networks and systems the contractor uses to destroy, maintain, receive, retain, or use VA information.

c. As part of these audits, tests and assessments, the contractor shall provide all information requested by VA. This information includes, but is not limited to, the following: equipment lists, network or infrastructure diagrams, relevant policy documents, system logs or details on information systems accessing, transporting, or processing VA data.

d. The contractor and at its own expense, shall comply with any recommendations resulting from VA audits, inspections and tests. VA further retains the right to view any related security reports the contractor has generated as part of its own security assessment. The contractor shall also notify VA of the existence of any such security reports or other related assessments, upon completion and validation.

e. VA appointed auditors or other government agency partners may be granted access to such documentation on a need-to-know basis and coordinated through the COR/CO. The contractor shall comply with recommendations which result from these regulatory assessments on the part of VA regulators and associated government agency partners.

9. PRODUCT INTEGRITY, AUTHENTICITY, PROVENANCE, ANTI-COUNTERFEIT AND ANTI-TAMPERING. This entire section applies when the acquisition involves any product (application, hardware, or software) or when section 6 or 7 is included.

a. The contractor shall comply with Code of Federal Regulations (CFR) Title 15 Part 7, "Securing the Information and Communications Technology and Services (ICTS) Supply Chain", which prohibits ICTS Transactions from foreign adversaries. ICTS Transactions are defined as any acquisition, importation, transfer, installation, dealing in or use of any information and communications technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs or the platforming or data hosting of applications for consumer download.

b. When contracting terms require the contractor to procure equipment, the contractor shall purchase or acquire the equipment from an Original Equipment Manufacturer (OEM) or an authorized reseller of the OEM. The contractor shall attest that equipment procured from an OEM or authorized reseller or distributor is authentic. If procurement is unavailable from an OEM or authorized reseller, the contractor shall submit in writing details of the circumstances prohibiting this from happening and procure a product waiver from VA COR/CO.

c. All contractors shall establish, implement, and provide documentation for risk management practices for supply chain delivery of hardware, software (to include patches) and firmware provided under this agreement. Documentation will include chain of custody practices, inventory management program, information protection practices, integrity management program for sub-supplier provided components, and replacement parts requests. The contractor shall make spare parts available. All contractors(s) shall specify how digital delivery for procured products, including patches, will be validated and monitored to ensure consistent delivery. The contractor shall apply encryption technology to protect procured products throughout the delivery process.

d. If a contractor provides software or patches to VA, the contractor shall publish or provide a hash conforming to the FIPS Security Requirements for Cryptographic Modules (FIPS 140-2 or successor).

e. The contractor shall provide a software bill of materials (SBOM) for procured (to include licensed products) and consist of a list of components and associated metadata which make up the product. SBOMs must be generated in one of the data formats defined in the National Telecommunications and Information Administration (NTIA) report "The Minimum Elements for a Software Bill of Materials (SBOM)."

f. Contractors shall use or arrange for the use of trusted channels to ship procured products, such as U.S. registered mail and/or tamper-evident packaging for physical deliveries.

g. Throughout the delivery process, the contractor shall demonstrate a capability for detecting unauthorized access (tampering).

h. The contractor shall demonstrate chain-of-custody documentation for procured products and require tamper-evident packaging for the delivery of this hardware.

10. VIRUSES, FIRMWARE AND MALWARE. This entire section applies when the acquisition involves any product (application, hardware, or software) or when section 6 or 7 is included.

a. The contractor shall execute due diligence to ensure all software provided and patches, including third-party patches, are free of viruses and/or malware before releasing them to or installing them on VA information systems.

b. The contractor warrants it has no knowledge of and did not insert, any malicious virus and/or malware code into any software or patches provided to VA which could potentially harm or

disrupt VA information systems. The contractor shall use due diligence, if supplying third-party software or patches, to ensure the third-party has not inserted any malicious code and/or virus which could damage or disrupt VA information systems.

c. The contractor shall provide or arrange for the provision of technical justification as to why any "false positive" hit has taken place to ensure their code's supply chain has not been compromised. Justification may be required, but is not limited to when install files, scripts, firmware, or other contractor-delivered software solutions (including third-party install files, scripts, firmware, or other software) are flagged as malicious, infected, or suspicious by an anti-virus vendor.

d. The contractor shall not upload (intentionally or negligently) any virus, worm, malware or any harmful or malicious content, component and/or corrupted data/source code (hereinafter "virus or other malware") onto VA computer and information systems and/or networks. If introduced (and this clause is violated), upon written request from the VA CO, the contractor shall:

(1) Take all necessary actions to correct the incident, to include all assistance to VA to eliminate the virus or other malware throughout VA's information networks, computer systems and information systems; and

(2) Use commercially reasonable efforts to restore operational efficiency and remediate damage due to data loss or data integrity damage, if the virus or other malware causes a loss of operational efficiency, data loss, or damage to data integrity.

11. CRYPTOGRAPHIC REQUIREMENT. This entire section applies whenever the acquisition includes section 6 or 7 is included.

a. The contractor shall document how the cryptographic system supporting the contractor's products and/or services protect the confidentiality, data integrity, authentication and non-repudiation of devices and data flows in the underlying system.

b. The contractor shall use only approved cryptographic methods as defined in FIPS 140-2 (or its successor) and NIST 800-52 standards when enabling encryption on its products.

c. The contractor shall provide or arrange for the provision of an automated remote key-establishment method which protects the confidentiality and integrity of the cryptographic keys.

d. The contractor shall ensure emergency re-keying of all devices can be remotely performed within 30 business days.

e. The contractor shall provide or arrange for the provision of a method for updating cryptographic primitives or algorithms.

12. PATCHING GOVERNANCE. This entire section applies whenever the acquisition includes section 7 is included

a. The contractor provides documentation detailing patch management, vulnerability management, mitigation and updating processes (including third-party) prior to the connection of electronic devices, assets or equipment to VA's assets. This documentation will include information regarding the following:

(1) The resources and technical capabilities to sustain the program or process (e.g., how the integrity of a patch is validated by VA); and

(2) The approach and capability to remediate newly reported zero-day vulnerabilities for contractor products.

b. The contractor shall verify and provide documentation that all procured products (including third-party applications, hardware, software, operating systems, and firmware) have appropriate updates and patches installed prior to delivery to VA.

c. The contractor shall provide or arrange the provision of appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses for their products and services within 30 days of discovery. Updates to remediate critical or emergent vulnerabilities will be provided within seven business days of discovery. If updates cannot be made available by contractor within these time periods, the contractor shall submit mitigations, methods of exploit detection and/or workarounds to the COR/CO prior to the above deadlines.

d. The contractor shall provide or arrange for the provision of appropriate hardware, software and/or firmware updates, when those products, including open-source software, are provided to the VA, to remediate newly discovered vulnerabilities or weaknesses. Remediations of products or services provided to the VA's system environment must be provided within 30 business days of availability from the original supplier and/or patching source. Updates to remediate critical vulnerabilities applicable to the Contractor's use of the third-party product in its system environment will be provided within seven business days of availability from the original supplier and/or patching source. If applicable third-party updates cannot be integrated, tested and made available by Contractor within these time periods, mitigations and/or workarounds will be provided to the COR/CO before the above deadlines.

13. SPECIALIZED DEVICES/SYSTEMS (MEDICAL DEVICES, SPECIAL PURPOSE SYSTEMS, RESEARCH SCIENTIFIC COMPUTING). This entire section applies when the acquisition includes one or more Medical Device, Special Purpose System or Research Scientific Computing Device. If appropriate, ensure selected clauses from section 6 or 7 and 8 through 12 are included.

a. Contractor supplies/delivered Medical Devices, Special Purpose Systems-Operational Technology (SPS-OT) and Research Scientific Computing Devices shall comply with all applicable Federal law, regulations, and VA policies. New developments require creation, testing, evaluation, and authorization in compliance with processes specified on the Specialized Device Cybersecurity Department Enterprise Risk Management (SDCD-ERM) Portal, VA Directive 6550, Pre-Procurement Assessment and Implementation of Medical Devices/Systems, VA Handbook 6500, and the VA Information Security Knowledge Service. Deviations from Federal law, regulations, and VA Policy are identified and documented as part of VA Directive 6550 and/or the VA Enterprise Risk Analysis (ERA) processes for Specialized Devices/Systems processes.

b. All contractors and third-party service providers shall address and/or integrate applicable VA Handbook 6500 and Information Security Knowledge Service specifications in delivered IT systems/solutions, products and/or services. If systems/solutions, products and/or services do not directly match VA security requirements, the contractor shall work though the COR/CO for governance or resolution.

c. The contractor certifies to the COR/CO that devices/systems that have completed the VA Enterprise Risk Analysis (ERA) process for Specialized Devices/Systems are fully functional and operate correctly as intended. Devices/systems must follow the VA ERA authorized configuration prior to acquisition and connection to the VA computing environment. If VA determines a new VA ERA that needs to be created, the contractor shall provide required technical support to develop the configuration settings. Major changes to a previously approved device/system will require a new ERA.

d. The contractor shall comply with all practices documented by the Food Drug and Administration (FDA) Premarket Submission for Management of Cybersecurity in Medical Devices and Post market Management of Cybersecurity in Medical Devices.

e. The contractor shall design devices capable of accepting all applicable security patches with or without the support of the contractor personnel. If patching can only be completed by the contractor, the contractor shall commit the resources needed to patch all applicable devices at all VA locations. If unique patching instructions or packaging are needed, the contractor shall provide the necessary information in conjunction with the validation/testing of the patch. The contractor shall apply security patches within 30 business days of the patch release and have a formal tracking process for any security patches not implemented to include explanation when a device cannot be patched.

f. The contractor shall provide devices able to install and maintain VA-approved antivirus capabilities with the capability to quarantine files and be updated as needed in response to incidents. Alternatively, a VA-approved whitelisting application may be used when the contractor cannot install an anti-virus / anti-malware application.

g. The contractor shall verify and document all software embedded within the device which does not contain any known viruses or malware before delivery to our installation at a VA location.

h. Devices and other equipment or systems containing media (hard drives, optical disks, solid state, and storage via chips/firmware) with VA sensitive information will be returned to the contractor with media removed. When the contract requires return of equipment, the options available to the contractor are the following:

(1) The contractor shall accept the system without the drive, firmware and solid state.

(2) VA's initial device purchase includes a spare drive or other replacement media which must be installed in place of the original drive at time of turn-in; or

(3) Due to the highly specialized and sometimes proprietary hardware and software associated with the device, if it is not possible for VA to retain the hard drive, firmware, and solid state, then:

(a) The equipment contractor shall 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.

(b) Any fixed hard drive, Complementary Metal-Oxide-Semiconductor (CMOS), Programmable Read-Only Memory (PROM), solid state and firmware 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 pre-approved and described in the solicitation, contract, or order.

14. DATA CENTER PROVISIONS. This entire section applies whenever the acquisition requires an interconnection to/from the VA network to/from a non-VA location.

a. The contractor shall ensure the VA network is accessed in accordance with VA Directive 6500 and IAM security processes specified in the VA Information Security Knowledge Service.

b. The contractor shall ensure network infrastructure and data availability in accordance with VA information system business continuity procedures specified in the VA Information Security Knowledge Service.

c. The contractor shall ensure any connections to the internet or other external networks for information systems occur through managed interfaces utilizing VA approved boundary protection devices (e.g., internet proxies, gateways, routers, firewalls, guards or encrypted tunnels).

d. The contractor shall encrypt all traffic across the segment of the Wide Area Network (WAN) it manages, and no unencrypted Out of Band (OOB) Internet Protocol (IP) traffic will traverse the network.

e. The contractor shall ensure tunnel endpoints are routable addresses at each VA operating site.

f. The contractor shall secure access from Local Area Networks (LANs) at co-located sites in accordance with VA TIC Reference Architecture, VA Directive and Handbook 6513, and MOU/ISA process specified in the VA Information Security Knowledge Service.

RECORDS MANAGEMENT OBLIGATIONS

A. *Applicability*

This clause applies to all Contractors whose employees create, work with, or otherwise handle Federal records, as defined in Section B, regardless of the medium in which the record exists.

B. *Definitions*

“Federal record” as defined in 44 U.S.C. § 3301, includes all recorded formation, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.

The term Federal record:

1. includes Department of Veterans Affairs (VA) (Lt. Col. Luke Weathers Jr. VA Medical Center) records.

2. does not include personal materials.

3. applies to records created, received, or maintained by Contractors pursuant to their VA (Lt. Col. Luke Weathers Jr. VA Medical Center) contract.

4. may include deliverables and documentation associated with deliverables.

C. *Requirements*

1. Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.

2. In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

3. In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created while performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with

Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

4. The VA (Lt. Col. Luke Weathers Jr. VA Medical Center) and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of the VA (Lt. Col. Luke Weathers Jr. VA Medical Center) or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report to the VA (Lt. Col. Luke Weathers Jr. VA Medical Center). The agency must report promptly to NARA in accordance with 36 CFR 1230.

5. The Contractor shall immediately notify the appropriate Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records, or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the Statement of Work (SOW) or Performance Work Statement (PWS). The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment are properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government’s behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to the VAs (Lt. Col. Luke Weathers Jr. VA Medical Center) control, or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the Statement of Work (SOW) or Performance Work Statement (PWS). Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

6. The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any subcontractor) is required to abide by Government and the VAs (Lt. Col. Luke Weathers Jr. VA Medical Center) guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.

7. The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with the VAs (Lt. Col. Luke Weathers Jr. VA Medical Center) policy.

8. The Contractor shall not create or maintain any records containing any nonpublic VA (Lt. Col. Luke Weathers Jr. VA Medical Center) information that are not specifically tied to or authorized by the contract.

9. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

10. The VA (Lt. Col. Luke Weathers Jr. VA Medical Center) owns the rights to all data and records produced as part of this contract. All deliverables under the contracts are the property of the U.S. Government for which the VA (Lt. Col. Luke Weathers Jr. VA Medical Center) shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.

11. Training. All Contractor employees assigned to this contract who create, work with, or otherwise handle records are required to take VA-provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

[Note: To the extent an agency requires contractors to complete records management training, the agency must provide the training to the contractor.]

D. *Flow down of requirements to subcontractors*

1. The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this Statement of Work (SOW) or Performance Work Statement (PWS) and require written subcontractor acknowledgment of same.

2. Violation by a subcontractor of any provision set forth in this clause will be attributed to the Contractor.

"The Authorization requirements do not apply, and that a Security Accreditation Package is not required."