

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 of 1974 (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 to not affecting the Systems within 10 business days.

B7. 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, change 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.) on 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 assessment 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 a 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) need(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.

B8. 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.

B9. 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 are 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 the 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 contractor(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.

B10. 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 provided software 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 action to correct the incident, to include any and 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 damages 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.

B11. 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.

B12. PATCHING GOVERNANCE.

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

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

B13. 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 through the COR/CO for governance or resolution.
- c. The contractor shall certify 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 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 is 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 does not contain any known viruses or malware before delivery to or 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:
 - b) 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.

B14. 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 by 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.

SECTION C - CONTRACT CLAUSES

C.1 52.212-4 CONTRACT TERMS AND CONDITIONS—COMMERCIAL ITEMS (JAN 2017)

(a) *Inspection/Acceptance.* The Contractor shall only tender for acceptance those items that conform to the requirements of this contract. The Government reserves the right to inspect or test any supplies or services that have been tendered for acceptance. The Government may require repair or replacement of nonconforming supplies or reperformance of nonconforming services at no increase in contract price. If repair/replacement or reperformance will not correct the defects or is not possible, the Government may seek an equitable price reduction or adequate consideration for acceptance of nonconforming supplies or services. The Government must exercise its post-acceptance rights—

(1) Within a reasonable time after the defect was discovered or should have been discovered; and

(2) Before any substantial change occurs in the condition of the item, unless the change is due to the defect in the item.

Notwithstanding the foregoing, use of the item in production will constitute acceptance by the VA.

(b) *Assignment.* The Contractor or its assignee may assign its rights to receive payment due as a result of performance of this contract to a bank, trust company, or other financing institution, including any Federal lending agency in accordance with the Assignment of Claims Act (31 U.S.C. 3727). However, when a third party makes payment (e.g., use of the Governmentwide commercial purchase card), the Contractor may not assign its rights to receive payment under this contract.

(c) *Changes.* Changes in the terms and conditions of this contract may be made only by written agreement of the parties.

(d) *Disputes.* This contract is subject to 41 U.S.C. chapter 71, Contract Disputes. Failure of the parties to this contract to reach agreement on any request for equitable adjustment, claim, appeal or action arising under or relating to this contract shall be a dispute to be resolved in accordance with the clause at FAR 52.233-1, Disputes, which is incorporated herein by reference. The Contractor shall proceed diligently with performance of this contract, pending final resolution of any dispute arising under the contract.

(e) *Definitions.* The clause at FAR 52.202-1, Definitions, is incorporated herein by reference.

(f) *Excusable delays.* The Contractor shall be liable for default unless nonperformance is caused by an occurrence beyond the reasonable control of the Contractor and

without its fault or negligence such as, acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. The Contractor shall notify the Contracting Officer in writing as soon as it is reasonably possible after the commencement of any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch, and shall promptly give written notice to the Contracting Officer of the cessation of such occurrence.

(g) Invoice.

(1) The Contractor shall submit an original invoice and three copies (or electronic invoice, if authorized) to the address designated in the contract to receive invoices. An invoice must include—

(i) Name and address of the Contractor;

(ii) Invoice date and number;

(iii) Contract number, line item number and, if applicable, the order number;

(iv) Description, quantity, unit of measure, unit price and extended price of the items delivered;

(v) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;

(vi) Terms of any discount for prompt payment offered;

(vii) Name and address of official to whom payment is to be sent;

(viii) Name, title, and phone number of person to notify in event of defective invoice; and

(ix) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract.

(x) Electronic funds transfer (EFT) banking information.

(A) The Contractor shall include EFT banking information on the invoice only if required elsewhere in this contract.

(B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with the applicable solicitation provision, contract clause (e.g., 52.232-33, Payment by Electronic Funds Transfer—System for Award Management, or 52.232-34, Payment by Electronic Funds Transfer—Other Than System for Award Management), or applicable agency procedures.

(C) EFT banking information is not required if the Government waived the requirement to pay by EFT.

(2) Invoices will be handled in accordance with the Prompt Payment Act (31 U.S.C. 3903) and Office of Management and Budget (OMB) prompt payment regulations at 5 CFR part 1315.

(h) *Patent indemnity.* The Contractor shall indemnify the Government and its officers, employees and agents against liability, including costs, for actual or alleged direct or contributory infringement of, or inducement to infringe, any United States or foreign patent, trademark or copyright, arising out of the performance of this contract, provided the Contractor is reasonably notified of such claims and proceedings.

(i) *Payment.*—

(1) *Items accepted.* Payment shall be made for items accepted by the Government that have been delivered to the delivery destinations set forth in this contract.

(2) *Prompt payment.* The Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations at 5 CFR part 1315.

(3) *Electronic Funds Transfer (EFT).* If the Government makes payment by EFT, see 52.212-5(b) for the appropriate EFT clause.

(4) *Discount.* In connection with any discount offered for early payment, time shall be computed from the date of the invoice. For the purpose of computing the discount earned, payment shall be considered to have been made on the date which appears on the payment check or the specified payment date if an electronic funds transfer payment is made.

(5) *Overpayments.* If the Contractor becomes aware of a duplicate contract financing or invoice payment or that the Government has otherwise overpaid on a contract financing or invoice payment, the Contractor shall—

(i) Remit the overpayment amount to the payment office cited in the contract along with a description of the overpayment including the—

(A) Circumstances of the overpayment (e.g., duplicate payment, erroneous payment, liquidation errors, date(s) of overpayment);

(B) Affected contract number and delivery order number, if applicable;

(C) Affected line item or subline item, if applicable; and

(D) Contractor point of contact.

(ii) Provide a copy of the remittance and supporting documentation to the Contracting Officer.

(6) *Interest.*

(i) All amounts that become payable by the Contractor to the Government under this contract shall bear simple interest from the date due until paid unless paid within 30 days of becoming due. The interest rate shall be the interest rate established by the Secretary of the Treasury as provided in 41 U.S.C. 7109, which is applicable to the period in which the amount becomes due, as provided in (i)(6)(v) of this clause, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid.

(ii) The Government may issue a demand for payment to the Contractor upon finding a debt is due under the contract.

(iii) *Final decisions.* The Contracting Officer will issue a final decision as required by 33.211 if—

(A) The Contracting Officer and the Contractor are unable to reach agreement on the existence or amount of a debt within 30 days;

(B) The Contractor fails to liquidate a debt previously demanded by the Contracting Officer within the timeline specified in the demand for payment unless the amounts were not repaid because the Contractor has requested an installment payment agreement; or

(C) The Contractor requests a deferment of collection on a debt previously demanded by the Contracting Officer (see 32.607-2).

(iv) If a demand for payment was previously issued for the debt, the demand for payment included in the final decision shall identify the same due date as the original demand for payment.

(v) Amounts shall be due at the earliest of the following dates:

(A) The date fixed under this contract.

(B) The date of the first written demand for payment, including any demand for payment resulting from a default termination.

(vi) The interest charge shall be computed for the actual number of calendar days involved beginning on the due date and ending on—

(A) The date on which the designated office receives payment from the Contractor;

(B) The date of issuance of a Government check to the Contractor from which an amount otherwise payable has been withheld as a credit against the contract debt; or

(C) The date on which an amount withheld and applied to the contract debt would otherwise have become payable to the Contractor.

(vii) The interest charge made under this clause may be reduced under the procedures prescribed in 32.608-2 of the Federal Acquisition Regulation in effect on the date of this contract.

(j) *Risk of loss.* Unless the contract specifically provides otherwise, risk of loss or damage to the supplies provided under this contract shall remain with the Contractor until, and shall pass to the Government upon:

(1) Delivery of the supplies to a carrier, if transportation is f.o.b. origin; or

(2) Delivery of the supplies to the Government at the destination specified in the contract, if transportation is f.o.b. destination.

(k) *Taxes.* The contract price includes all applicable Federal, State, and local taxes and duties.

(l) *Termination for the Government's convenience.* The Government reserves the right to terminate this contract, or any part hereof, for its sole convenience. In the event of such termination, the Contractor shall immediately stop all work hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of this contract, the Contractor shall be paid a percentage of the contract price reflecting the percentage of the work performed prior to the notice of termination, plus reasonable charges the Contractor can demonstrate to the satisfaction of the Government using its standard record keeping system, have resulted from the termination. The Contractor shall not be required to comply with the cost accounting standards or contract cost principles for this purpose. This paragraph does not give the Government any right to audit the Contractor's records. The Contractor shall not be paid for any work performed or costs incurred which reasonably could have been avoided.

(m) *Termination for cause.* The Government may terminate this contract, or any part hereof, for cause in the event of any default by the Contractor, or if the Contractor fails to comply with any contract terms and conditions, or fails to provide the Government, upon request, with adequate assurances of future performance. In the event of termination for cause, the Government shall not be liable to the Contractor for any amount for supplies or services not accepted, and the Contractor shall be liable to the Government for any and all rights and remedies provided by law. If it is determined that the Government improperly terminated this contract for default, such termination shall be deemed a termination for convenience.

(n) *Title.* Unless specified elsewhere in this contract, title to items furnished under this contract shall pass to the Government upon acceptance, regardless of when or where the Government takes physical possession.

(o) *Warranty.* The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract.

(p) *Limitation of liability.* Except as otherwise provided by an express warranty, the Contractor will not be liable to the Government for consequential damages resulting from any defect or deficiencies in accepted items.

(q) *Other compliances.* The Contractor shall comply with all applicable Federal, State and local laws, executive orders, rules and regulations applicable to its performance under this contract.

(r) *Compliance with laws unique to Government contracts.* The Contractor agrees to comply with 31 U.S.C. 1352 relating to limitations on the use of appropriated funds to influence certain Federal contracts; 18 U.S.C. 431 relating to officials not to benefit; 40 U.S.C. chapter 37, Contract Work Hours and Safety Standards; 41 U.S.C. chapter 87, Kickbacks; 41 U.S.C. 4712 and 10 U.S.C. 2409 relating to whistleblower protections; 49 U.S.C. 40118, Fly American; and 41 U.S.C. chapter 21 relating to procurement integrity.

(s) *Order of precedence.* Any inconsistencies in this solicitation or contract shall be resolved by giving precedence in the following order:

(1) The schedule of supplies/services.

(2) The Assignments, Disputes, Payments, Invoice, Other Compliances, Compliance with Laws Unique to Government Contracts, and Unauthorized Obligations paragraphs of this clause;

(3) The clause at 52.212-5.

(4) Addenda to this solicitation or contract, including any license agreements for computer software.

(5) Solicitation provisions if this is a solicitation.

(6) Other paragraphs of this clause.

(7) The Standard Form 1449.

(8) Other documents, exhibits, and attachments

(9) The specification.

(t) *System for Award Management (SAM).*

(1) Unless exempted by an addendum to this contract, the Contractor is responsible during performance and through final payment of any contract for the accuracy and completeness of the data within the SAM database, and for any liability resulting from the Government's reliance on inaccurate or incomplete data. To remain registered in the

SAM database after the initial registration, the Contractor is required to review and update on an annual basis from the date of initial registration or subsequent updates its information in the SAM database to ensure it is current, accurate and complete. Updating information in the SAM does not alter the terms and conditions of this contract and is not a substitute for a properly executed contractual document.

(2)(i) If a Contractor has legally changed its business name, "doing business as" name, or division name (whichever is shown on the contract), or has transferred the assets used in performing the contract, but has not completed the necessary requirements regarding novation and change-of-name agreements in FAR subpart 42.12, the Contractor shall provide the responsible Contracting Officer a minimum of one business day's written notification of its intention to (A) change the name in the SAM database; (B) comply with the requirements of subpart 42.12; and (C) agree in writing to the timeline and procedures specified by the responsible Contracting Officer. The Contractor must provide with the notification sufficient documentation to support the legally changed name.

(ii) If the Contractor fails to comply with the requirements of paragraph (t)(2)(i) of this clause, or fails to perform the agreement at paragraph (t)(2)(i)(C) of this clause, and, in the absence of a properly executed novation or change-of-name agreement, the SAM information that shows the Contractor to be other than the Contractor indicated in the contract will be considered to be incorrect information within the meaning of the "Suspension of Payment" paragraph of the electronic funds transfer (EFT) clause of this contract.

(3) The Contractor shall not change the name or address for EFT payments or manual payments, as appropriate, in the SAM record to reflect an assignee for the purpose of assignment of claims (see Subpart 32.8, Assignment of Claims). Assignees shall be separately registered in the SAM database. Information provided to the Contractor's SAM record that indicates payments, including those made by EFT, to an ultimate recipient other than that Contractor will be considered to be incorrect information within the meaning of the "Suspension of payment" paragraph of the EFT clause of this contract.

(4) Offerors and Contractors may obtain information on registration and annual confirmation requirements via SAM accessed through <https://www.acquisition.gov>.

(u) Unauthorized Obligations.

(1) Except as stated in paragraph (u)(2) of this clause, when any supply or service acquired under this contract is subject to any End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement, that includes any clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

(i) Any such clause is unenforceable against the Government.

(ii) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or agreement is invoked through an "I agree" click box or other comparable mechanism (e.g., "click-wrap" or "browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such clause.

(iii) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.

(2) Paragraph (u)(1) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

(v) *Incorporation by reference.* The Contractor's representations and certifications, including those completed electronically via the System for Award Management (SAM), are incorporated by reference into the contract.

(End of Clause)

ADDENDUM to FAR 52.212-4 CONTRACT TERMS AND CONDITIONS— COMMERCIAL ITEMS

Clauses that are incorporated by reference (by Citation Number, Title, and Date), have the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available.

The following clauses are incorporated into 52.212-4 as an addendum to this contract:

C.2 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

<http://www.acquisition.gov/far/index.html>

<http://www.va.gov/oamm/oa/ars/policyreg/vaar/index.cfm>

<u>FAR</u> <u>Number</u>	<u>Title</u>	<u>Date</u>
52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS	APR 2014

	PROHIBITION ON CONTRACTING WITH ENTITIES THAT REQUIRE CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS (DEVIATION)	FEB 2015
52.204-4	PRINTED OR COPIED DOUBLE-SIDED ON RECYCLED PAPER	MAY 2011
52.204-18	COMMERCIAL AND GOVERNMENT ENTITY CODE MAINTENANCE	JUL 2016
52.219-8	UTILIZATION OF SMALL BUSINESS CONCERNS	OCT 2014
52.227-1	AUTHORIZATION AND CONSENT	DEC 2007
52.227-2	NOTICE AND ASSISTANCE REGARDING PATENT AND COPYRIGHT INFRINGEMENT	DEC 2007
52.227-14	RIGHTS IN DATA—GENERAL	MAY 2014
52.227-17	RIGHTS IN DATA—SPECIAL WORKS	DEC 2007
52.232-40	PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS	DEC 2013

(End of Clause)

C.3 52.204-21 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (JUN 2016)

(a) *Definitions.* As used in this clause—

Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.

Information means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

Safeguarding means measures or controls that are prescribed to protect information systems.

(b) *Safeguarding requirements and procedures.* (1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor

information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

- (i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- (ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
- (iii) Verify and control/limit connections to and use of external information systems.
- (iv) Control information posted or processed on publicly accessible information systems.
- (v) Identify information system users, processes acting on behalf of users, or devices.
- (vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- (vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
- (viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
- (ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
- (x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- (xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
- (xii) Identify, report, and correct information and information system flaws in a timely manner.
- (xiii) Provide protection from malicious code at appropriate locations within organizational information systems.
- (xiv) Update malicious code protection mechanisms when new releases are available.
- (xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(2) *Other requirements.* This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(c) *Subcontracts.* The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

(End of Clause)

C.4 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 10 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 24 months.

(End of Clause)

C.5 VAAR 852.203-70 COMMERCIAL ADVERTISING (JAN 2008)

The bidder or offeror agrees that if a contract is awarded to him/her, as a result of this solicitation, he/she will not advertise the award of the contract in his/her commercial advertising in such a manner as to state or imply that the Department of Veterans Affairs endorses a product, project or commercial line of endeavor.

(End of Clause)

C.6 VAAR 852.232-72 ELECTRONIC SUBMISSION OF PAYMENT REQUESTS (NOV 2012)

(a) *Definitions.* As used in this clause—

(1) *Contract financing payment* has the meaning given in FAR 32.001.

(2) *Designated agency office* has the meaning given in 5 CFR 1315.2(m).

(3) *Electronic form* means an automated system transmitting information electronically according to the

Accepted electronic data transmission methods and formats identified in paragraph (c) of this clause. Facsimile, email, and scanned documents are not acceptable electronic forms for submission of payment requests.

(4) *Invoice payment* has the meaning given in FAR 32.001.

(5) *Payment request* means any request for contract financing payment or invoice payment submitted by the contractor under this contract.

(b) *Electronic payment requests.* Except as provided in paragraph (e) of this clause, the contractor shall submit payment requests in electronic form. Purchases paid with a Government-wide commercial purchase card are considered to be an electronic transaction for purposes of this rule, and therefore no additional electronic invoice submission is required.

(c) *Data transmission.* A contractor must ensure that the data transmission method and format are through one of the following:

(1) VA's Electronic Invoice Presentment and Payment System. (See Web site at <http://www.fsc.va.gov/einvoice.asp>.)

(2) Any system that conforms to the X12 electronic data interchange (EDI) formats established by the Accredited Standards Center (ASC) and chartered by the American National Standards Institute (ANSI). The X12 EDI Web site (<http://www.x12.org>) includes additional information on EDI 810 and 811 formats.

(d) *Invoice requirements.* Invoices shall comply with FAR 32.905.

(e) *Exceptions.* If, based on one of the circumstances below, the contracting officer directs that payment requests be made by mail, the contractor shall submit payment requests by mail through the United States Postal Service to the designated agency office. Submission of payment requests by mail may be required for:

(1) Awards made to foreign vendors for work performed outside the United States;

(2) Classified contracts or purchases when electronic submission and processing of payment requests could compromise the safeguarding of classified or privacy information;

(3) Contracts awarded by contracting officers in the conduct of emergency operations, such as responses to national emergencies;

(4) Solicitations or contracts in which the designated agency office is a VA entity other than the VA Financial Services Center in Austin, Texas; or

(5) Solicitations or contracts in which the VA designated agency office does not have electronic invoicing capability as described above.

(End of Clause)

C.7 VAAR 852.237-70 CONTRACTOR RESPONSIBILITIES (APR 1984)

The contractor shall obtain all necessary licenses and/or permits required to perform this work. He/she shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract. He/she shall be responsible for any injury to himself/herself, his/her employees, as well as for any damage to personal or public property that occurs during the performance of this contract that is caused by his/her employees fault or negligence, and shall maintain personal liability and property damage insurance having coverage for a limit as required by the laws of the State of the state in which the majority of the work will take place. Further, it is agreed that any negligence of the Government, its officers, agents, servants and employees, shall not be the responsibility of the contractor hereunder with the regard to any claims, loss, damage, injury, and liability resulting there from.

(End of Clause)

C.8 VAAR 852.270-1 REPRESENTATIVES OF CONTRACTING OFFICERS (JAN 2008)

The contracting officer reserves the right to designate representatives to act for him/her in furnishing technical guidance and advice or generally monitor the work to be performed under this contract. Such designation will be in writing and will define the scope and limitation of the designee's authority. A copy of the designation shall be furnished to the contractor.

(End of Clause)

C.9 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS—COMMERCIAL ITEMS (JAN 2018)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(2) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (NOV 2015).

(3) 52.233-3, Protest After Award (Aug 1996) (31 U.S.C. 3553).

(4) 52.233-4, Applicable Law for Breach of Contract Claim (Oct 2004) (Public Laws 108-77 and 108-78 (19 U.S.C. 3805 note)).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

☒ (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).

☒ (2) 52.203-13, Contractor Code of Business Ethics and Conduct (OCT 2015) (41 U.S.C. 3509).

☐ (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (JUN 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)

☒ (4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (OCT 2016) (Pub. L. 109-282) (31 U.S.C. 6101 note).

☐ (5) [Reserved]

☒ (6) 52.204-14, Service Contract Reporting Requirements (OCT 2016) (Pub. L. 111-117, section 743 of Div. C).

☐ (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (OCT 2016) (Pub. L. 111-117, section 743 of Div. C).

☒ (8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (OCT 2015) (31 U.S.C. 6101 note).

☐ (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Jul 2013) (41 U.S.C. 2313).

☐ (10) [Reserved]

☐ (11)(i) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (NOV 2011) (15 U.S.C. 657a).

☐ (ii) Alternate I (NOV 2011) of 52.219-3.

☐ (12)(i) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (OCT 2014) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).

☐ (ii) Alternate I (JAN 2011) of 52.219-4.

- ☐ (13) [Reserved]
- ☐ (14)(i) 52.219-6, Notice of Total Small Business Set-Aside (NOV 2011) (15 U.S.C. 644).
- ☐ (ii) Alternate I (NOV 2011).
- ☐ (iii) Alternate II (NOV 2011).
- ☐ (15)(i) 52.219-7, Notice of Partial Small Business Set-Aside (June 2003) (15 U.S.C. 644).
- ☐ (ii) Alternate I (Oct 1995) of 52.219-7.
- ☐ (iii) Alternate II (Mar 2004) of 52.219-7.
- ☒ (16) 52.219-8, Utilization of Small Business Concerns (NOV 2016) (15 U.S.C. 637(d)(2) and (3)).
- ☐ (17)(i) 52.219-9, Small Business Subcontracting Plan (JAN 2017) (15 U.S.C. 637(d)(4)).
- ☐ (ii) Alternate I (NOV 2016) of 52.219-9.
- ☐ (iii) Alternate II (NOV 2016) of 52.219-9.
- ☐ (iv) Alternate III (NOV 2016) of 52.219-9.
- ☐ (v) Alternate IV (NOV 2016) of 52.219-9.
- ☐ (18) 52.219-13, Notice of Set-Aside of Orders (NOV 2011) (15 U.S.C. 644(r)).
- ☐ (19) 52.219-14, Limitations on Subcontracting (JAN 2017) (15 U.S.C. 637(a)(14)).
- ☐ (20) 52.219-16, Liquidated Damages—Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).
- ☐ (21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (NOV 2011) (15 U.S.C. 657f).
- ☒ (22) 52.219-28, Post Award Small Business Program Rerepresentation (Jul 2013) (15 U.S.C. 632(a)(2)).
- ☐ (23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (DEC 2015) (15 U.S.C. 637(m)).
- ☐ (24) 52.219-30, Notice of Set-Aside for, or Sole Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (DEC 2015) (15 U.S.C. 637(m)).

- [x] (25) 52.222-3, Convict Labor (June 2003) (E.O. 11755).
- [x] (26) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (JAN 2018) (E.O. 13126).
- [x] (27) 52.222-21, Prohibition of Segregated Facilities (APR 2015).
- [x] (28) 52.222-26, Equal Opportunity (SEP 2016) (E.O. 11246).
- [x] (29) 52.222-35, Equal Opportunity for Veterans (OCT 2015) (38 U.S.C. 4212).
- [x] (30) 52.222-36, Equal Opportunity for Workers with Disabilities (JUL 2014) (29 U.S.C. 793).
- [x] (31) 52.222-37, Employment Reports on Veterans (FEB 2016) (38 U.S.C. 4212).
- [x] (32) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496).
- [x] (33)(i) 52.222-50, Combating Trafficking in Persons (MAR 2015) (22 U.S.C. chapter 78 and E.O. 13627).
- ☐ (ii) Alternate I (MAR 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).
- ☐ (34) 52.222-54, Employment Eligibility Verification (OCT 2015). (E. O. 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)
- ☐ (35)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
- ☐ (ii) Alternate I (MAY 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
- ☐ (36) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (JUN 2016) (E.O. 13693).
- ☐ (37) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (JUN 2016) (E.O. 13693).
- ☐ (38)(i) 52.223-13, Acquisition of EPEAT®-Registered Imaging Equipment (JUN 2014) (E.O.s 13423 and 13514).
- ☐ (ii) Alternate I (OCT 2015) of 52.223-13.
- ☐ (39)(i) 52.223-14, Acquisition of EPEAT®-Registered Televisions (JUN 2014) (E.O.s 13423 and 13514).

- ☐ (ii) Alternate I (JUN 2014) of 52.223-14.
- ☐ (40) 52.223-15, Energy Efficiency in Energy-Consuming Products (DEC 2007)(42 U.S.C. 8259b).
- ☐ (41)(i) 52.223-16, Acquisition of EPEAT®-Registered Personal Computer Products (OCT 2015) (E.O.s 13423 and 13514).
- ☐ (ii) Alternate I (JUN 2014) of 52.223-16.
- ☒ (42) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (AUG 2011)
- ☐ (43) 52.223-20, Aerosols (JUN 2016) (E.O. 13693).
- ☐ (44) 52.223-21, Foams (JUN 2016) (E.O. 13693).
- ☒ (45) (i) 52.224-3, Privacy Training (JAN 2017) (5 U.S.C. 552a).
- ☐ (ii) Alternate I (JAN 2017) of 52.224-3.
- ☐ (46) 52.225-1, Buy American—Supplies (MAY 2014) (41 U.S.C. chapter 83).
- ☐ (47)(i) 52.225-3, Buy American—Free Trade Agreements—Israeli Trade Act (MAY 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).
- ☐ (ii) Alternate I (MAY 2014) of 52.225-3.
- ☐ (iii) Alternate II (MAY 2014) of 52.225-3.
- ☐ (iv) Alternate III (MAY 2014) of 52.225-3.
- ☐ (48) 52.225-5, Trade Agreements (OCT 2016) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).
- ☒ (49) 52.225-13, Restrictions on Certain Foreign Purchases (JUN 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).
- ☐ (50) 52.225-26, Contractors Performing Private Security Functions Outside the United States (OCT 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
- ☐ (51) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

☐ (52) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).

☐ (53) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

☐ (54) 52.232-30, Installment Payments for Commercial Items (JAN 2017) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

☒ (55) 52.232-33, Payment by Electronic Funds Transfer—System for Award Management (Jul 2013) (31 U.S.C. 3332).

☐ (56) 52.232-34, Payment by Electronic Funds Transfer—Other than System for Award Management (Jul 2013) (31 U.S.C. 3332).

☐ (57) 52.232-36, Payment by Third Party (MAY 2014) (31 U.S.C. 3332).

☒ (58) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

☒ (59) 52.242-5, Payments to Small Business Subcontractors (JAN 2017)(15 U.S.C. 637(d)(12)).

☐ (60)(i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631).

☐ (ii) Alternate I (Apr 2003) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

☐ (1) 52.222-17, Nondisplacement of Qualified Workers (MAY 2014) (E.O. 13495).

☐ (2) 52.222-41, Service Contract Labor Standards (MAY 2014) (41 U.S.C. chapter 67).

☐ (3) 52.222-42, Statement of Equivalent Rates for Federal Hires (MAY 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

☐ (4) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards—Price Adjustment (Multiple Year and Option Contracts) (MAY 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

☐ (5) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards—Price Adjustment (MAY 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

□ (6) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment—Requirements (MAY 2014) (41 U.S.C. chapter 67).

□ (7) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Requirements (MAY 2014) (41 U.S.C. chapter 67).

□ (8) 52.222-55, Minimum Wages Under Executive Order 13658 (DEC 2015).

□ (9) 52.222-62, Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

□ (10) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (MAY 2014) (42 U.S.C. 1792).

□ (11) 52.237-11, Accepting and Dispensing of \$1 Coin (SEP 2008) (31 U.S.C. 5112(p)(1)).

(d) Comptroller General Examination of Record. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records—Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless

otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (OCT 2015) (41 U.S.C. 3509).

(ii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(iii) 52.219-8, Utilization of Small Business Concerns (NOV 2016) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities.

(iv) 52.222-17, Nondisplacement of Qualified Workers (MAY 2014) (E.O. 13495). Flow down required in accordance with paragraph (l) of FAR clause 52.222-17.

(v) 52.222-21, Prohibition of Segregated Facilities (APR 2015).

(vi) 52.222-26, Equal Opportunity (SEP 2016) (E.O. 11246).

(vii) 52.222-35, Equal Opportunity for Veterans (OCT 2015) (38 U.S.C. 4212).

(viii) 52.222-36, Equal Opportunity for Workers with Disabilities (JUL 2014) (29 U.S.C. 793).

(ix) 52.222-37, Employment Reports on Veterans (FEB 2016) (38 U.S.C. 4212).

(x) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(xi) 52.222-41, Service Contract Labor Standards (MAY 2014) (41 U.S.C. chapter 67).

(xii)(A) 52.222-50, Combating Trafficking in Persons (MAR 2015) (22 U.S.C. chapter 78 and E.O. 13627).

(B) Alternate I (MAR 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).

(xiii) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment—Requirements (MAY 2014) (41 U.S.C. chapter 67).

(xiv) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Requirements (MAY 2014) (41 U.S.C. chapter 67).

(xv) 52.222-54, Employment Eligibility Verification (OCT 2015) (E. O. 12989).

(xvi) 52.222-55, Minimum Wages Under Executive Order 13658 (DEC 2015).

(xvii) 52.222-62 Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

(xviii)(A) 52.224-3, Privacy Training (JAN 2017) (5 U.S.C. 552a).

(B) Alternate I (JAN 2017) of 52.224-3.

(xix) 52.225-26, Contractors Performing Private Security Functions Outside the United States (OCT 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xx) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (MAY 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xxi) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the Contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of Clause)

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS\

D.1 - Business Associate Agreement.

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 contract 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 perform 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 contractor.
- 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 with 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 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 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.
 - li. 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.
 - lii. 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.
 - liii. Any media, such as paper, magnetic tape, magnetic disks, solid state devices or optical discs that is 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.
 - liv. 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 the 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 a 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 has a need for access to VA information or VA information systems.
 - (6) Contractor/subcontractor personnel are terminated, suspended, or otherwise has their work on a VA project discontinued for any reason.
 - (6) Contractor believes 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.
 - (6) 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.
 - (6) 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 accesses 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.
 - (3) 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 to the COR/CO 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 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:
 - (6) The date and time (or approximation of) the Security Incident occurred.
 - (6) The names of individuals involved (when applicable).
 - (6) The physical and logical (if applicable) location of the incident.
 - (6) Why the Security Incident took place (i.e., catalyst for the failure).
 - (6) The amount of data belonging to VA 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 employees 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.
- ci. 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.
- cii. 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 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.
- ciii. 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.
- civ. 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.
- cv. 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 an Authority to Operate (ATO). VA Directive 6517, Risk Management Framework for Cloud Computing Services, provides the 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 through 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 contractor 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 of 1974 (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.
- li. 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.
- lii. 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 to 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, change 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.) on 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.
- ci. 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).
- cii. 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.

- ciii. 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.
- civ. 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 assessment 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 a 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) need(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 are 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 the 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 contractor(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 provided software 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:
 - (2) Take all necessary action to correct the incident, to include any and 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 damages 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 shall provide documentation detailing the patch management, vulnerability management, mitigation and update processes (to include third-party) prior to the connection of electronic devices, assets or equipment to VA's assets. This documentation will include information regarding the follow:
 - (2) 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 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 through the COR/CO for governance or resolution.
- c. The contractor shall certify 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 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 Postmarket 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 is 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 does not contain any known viruses or malware before delivery to or 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:
 - (3) The contractor shall accept the system without the drive, firmware and solid state.
 - (3) 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:
 - (b) 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 by 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.