SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NO.	PAGE 1 OF 69
636-26-4-4154-0232	

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NO.	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
			36C26326Q0899	

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NO. (No Collect Calls)	8. OFFER DUE DATE/LOCAL TIME
	Mark Clayburne	319-688-3625	07-31-2026 10:00 AM CDT

9. ISSUED BY	CODE	10. THIS ACQUISITION IS
DEPARTMENT OF VETERANS AFFAIRS NETWORK CONTRACTING OFFICE 23 1303 5TH STREET, SUITE 300 CORALVILLE IA 52241	36C263	☐ UNRESTRICTED OR ☒ SET ASIDE: 100 % FOR: ☐ SMALL BUSINESS ☐ HUBZONE SMALL BUSINESS ☒ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS ☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM ☐ EDWOSB ☐ 8(A) NAICS: 339113 SIZE STANDARD: 800 Employees

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING	14. METHOD OF SOLICITATION
☐ SEE SCHEDULE		☐	N/A	☒ RFQ ☐ IFB ☐ RFP

15. DELIVER TO	CODE	16. ADMINISTERED BY	CODE
DEPARTMENT OF VETERANS AFFAIRS Iowa City VA Medical Center 601 Highway 6 West Iowa City, IA 52246	36C636A8	DEPARTMENT OF VETERANS AFFAIRS NETWORK CONTRACTING OFFICE 23 1303 5TH STREET, SUITE 300 CORALVILLE IA 52241	36C263

17a. CONTRACTOR/OFFEROR CODE	FACILITY CODE	18a. PAYMENT WILL BE MADE BY	CODE
		DEPARTMENT OF VETERANS AFFAIRS FMS-VA-2(101) FINANCIAL SERVICES CENTER PO BOX 149971 AUSTIN TX 78714-9971	

TELEPHONE NO. UEI: EFT:

PHONE: FAX:

☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED
☐ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES (See CONTINUATION Page)	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Medical Video Monitors for the Iowa City VA Medical Center. This is an SDVOSB Set-Aside. Offerors shall be registered at System for Award Management (SAM). www.sam.gov All questions must be in writing and emailed to Mark.Clayburne@va.gov no later than 10:00 AM CDT 07/24/2026. See attached Statement of Work for details. FOB Destination 30 Days ARO All offerors shall fill out the Buy American Certificate (BAA) and return with the quote. Failure to sign the BAA will result in the quote being unresponsive. Offerors shall fill out the certification of compliance for limitations on subcontracting (LOS) at C.4 and return with quote. Failure to sign LOS form will result in quote being unresponsive. (Use Reverse and/or Attach Additional Sheets as Necessary)				

25. ACCOUNTING AND APPROPRIATION DATA (See CONTINUATION Page)
636-3660160-4154-822200-3131-0400K1043
636-26-4-4154-0232
636AXXX

26. TOTAL AWARD AMOUNT (For Govt. Use Only)

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☒ ARE ☐ ARE NOT ATTACHED.

☐ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED

☒ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 01 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED

☐ 29. AWARD OF CONTRACT: REF. _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR	31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)

30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT)	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT)	31c. DATE SIGNED
		Becky De Los Santos VA-VHA-RPOC-2025-0039	

Table of Contents

SECTION A 1

A.1 SF 1449 SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES 1

SECTION B - CONTINUATION OF SF 1449 BLOCKS 4

B.1 CONTRACT ADMINISTRATION DATA 4
B.2 STATEMENT OF WORK 5
B.3 RECORDS MANAGEMENT OBLIGATIONS 23
B.4 PRICE/COST SCHEDULE 26
ITEM INFORMATION 26
B.5 DELIVERY SCHEDULE 27

SECTION C - CONTRACT CLAUSES 28

C.1 52.212-4 CONTRACT TERMS AND CONDITIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (OCT 2025) (DEVIATION) 28
C.2 52.222-36 EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES (NOV 2025) (DEVIATION) 33
C.3 52.222-90 ADDRESSING DEI DISCRIMINATION BY FEDERAL CONTRACTORS (DEVIATION APR 2026) 33
C.4 52.223-23 SUSTAINABLE PRODUCTS (NOV 2025) (DEVIATION) 34
C.5 52.240-91 SECURITY PROHIBITIONS AND EXCLUSIONS (NOV 2025) (DEVIATION) 35
C.6 VAAR 852.219-73 VA NOTICE OF TOTAL SET-ASIDE FOR CERTIFIED SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESSES (JAN 2023) (DEVIATION) 45
C.7 VAAR 852.219-76 VA NOTICE OF LIMITATIONS ON SUBCONTRACTING—CERTIFICATE OF COMPLIANCE FOR SUPPLIES AND PRODUCTS (JAN 2023) (DEVIATION) 48
C.8 VAAR 852.247-73 PACKING FOR DOMESTIC SHIPMENT (OCT 2018) 50
C.9 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998) 50
52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998) 51

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS 52

SECTION E - SOLICITATION PROVISIONS 53

E.1 52.212-1 INSTRUCTIONS TO OFFERORS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (OCT 2025) (DEVIATION) 53
E.2 52.216-1 TYPE OF CONTRACT (NOV 2025) (DEVIATION) 54
E.3 52.225-1 BUY AMERICAN—SUPPLIES (NOV 2025) (DEVIATION) 54
E.4 52.225-3 BUY AMERICAN—FREE TRADE AGREEMENTS—ISRAELI TRADE ACT (DEVIATION) (NOV 2025) ALTERNATE III (DEVIATION) (NOV 2025) 57
E.5 52.225-4 BUY AMERICAN—FREE TRADE AGREEMENTS—ISRAELI TRADE ACT CERTIFICATE (DEVIATION) (NOV 2025) ALTERNATE II (JAN 2025) 60
E.6 52.225-5 TRADE AGREEMENTS (NOV 2023) 60
E.7 52.225-6 TRADE AGREEMENTS CERTIFICATE (FEB 2021) 63

E.8 52.240-90 SECURITY PROHIBITIONS AND EXCLUSIONS REPRESENTATIONS AND CERTIFICATIONS (NOV 2025) (DEVIATION).....64
E.9 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998).....68

SECTION B - CONTINUATION OF SF 1449 BLOCKS

B.1 CONTRACT ADMINISTRATION DATA

1. Contract Administration: All contract administration matters will be handled by the following individuals:

a. CONTRACTOR:

b. GOVERNMENT: Contracting Officer 36C263

DEPARTMENT OF VETERANS AFFAIRS

NETWORK CONTRACTING OFFICE 23

1303 5TH STREET, SUITE 300

CORALVILLE IA 52241

2. CONTRACTOR REMITTANCE ADDRESS: All payments by the Government to the contractor will be made in accordance with:

[] 52.232-33, Payment by Electronic Funds Transfer—System For Award Management, or
[] 52.232-36, Payment by Third Party

3. INVOICES: Invoices shall be submitted in arrears:

a. Quarterly []

b. Semi-Annually []

c. Other []

4. GOVERNMENT INVOICE ADDRESS: All Invoices from the contractor shall be submitted electronically in accordance with VAAR Clause 852.232-72 Electronic Submission of Payment Requests.

ACKNOWLEDGMENT OF AMENDMENTS: The offeror acknowledges receipt of amendments to the Solicitation numbered and dated as follows:

AMENDMENT NO	DATE

B.2 STATEMENT OF WORK

General Equipment Name: Patient Monitoring System

Description & Salient Characteristics
The Iowa City VA HCS MRI is requesting a Brand Name or Equal Medical Video Monitoring System to the Philips Magnetic Resonance (MR) Patient Care Portal 5000 compatible with existing equipment currently in use in the MRI department.

- Must have EMR/HIS Integration enabling electronic patient record-keeping.
- Must have 18.3”-18.5” touchscreen.
- Must have wireless capabilities.
- Must have AES 256 GCM encryption, compliant with IEC 80601 2 55 clinical alarm standards.
- Must be capable of remote printing.
- Must have Internal rechargeable battery, providing approx. 8 hours of runtime.
- Must have multi-tier visual/audio alarms with "alarm flags".
- Must have apnea, extreme bradycardia/tachycardia detection.
- Must have Built-in Gauss detection for MR environment safety.
- Desktop unit dimensions: H 7.57cm x W 19.06cm x D 17.87cm.
- Must be Certified safe for MRI environments: up to 3 Tesla, 5,000 Gauss static field, 7.2 µT B_1 rms, and 4 W/kg SAR.
- Must simultaneously support the monitoring of:
    - Wireless dual-channel ECG.
    - Wireless SpO_2
    - End-tidal/inspired CO_2
    - Non-invasive and invasive blood pressure (NIBP, IBP)
    - Respiratory rate, temperature, anesthetic agents (end-tidal/inspired N_2O & O_2, total MAC)
    - Up to 13 parameters and 6 waveform displays
- Must have remote MR monitoring and control.
    - Enables staff to remotely view/manage MRI patient monitoring system from the control room.

Technical Specifications:

- Rated for MRI environments up to 3 Tesla, 5,000 Gauss, 7.2 µT B_1 rms, 4 W/kg SAR
- Wireless dual-channel ECG (ECG 3.0)
- Wireless SpO_2
- Non-invasive blood pressure (NIBP)

- Invasive blood pressure (IBP)
- End-tidal and inspired CO_2
- Temperature
- Respiratory rate derived from CO_2 or bellows
- Anesthetic agents monitoring end-tidal/inspired N_2O, inspired O_2, total MAC
- Multi-priority visual/audio alarms
- “Alarm-flag” alerts for early condition changes
- Extreme tachycardia/bradycardia and apnea detection
- Gauss detection within MR field
- Bedside-level (“SINC”) accuracy for key parameters (SpO_2, IBP, NIBP, CO_2)
- Simultaneous display of up to 13 parameters and 6 waveforms
- Internal rechargeable battery, ≈8 hours runtime
- User-replaceable battery for continued use during MRI exams
- Traditional roll-around cart with integrated display
- Wireless sensor modules reduce cable clutter
- Expression Information Portal (IP5) support
- Remote printing and clinical data integration
- Network compatibility via HL7, RS-232, PIC iX, support for IntelliBridge Enterprise
- AES-256-GCM encryption, IEC 80601-2-55 compliance

Required Individual Line Items & Quantity of Items

- (2 each) MR Patient Care Portal
- (2 each) Standard Accessories
- (2 each) Patient Monitors
- (2 each) Remote Monitor
- (2 each) Desktop Unit
- (2 each) 18.5 Inch Display
- (2 each) MR400 2.0 Software Update

Optional Line Items

- Delivery Requirements:
    - All products should be ordered to arrive on or about August 18, 2026. Please include any shipping costs that are not included in the cost of the line items.

Required Training

- TMS 20939 No Access

INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE

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 R*ights in Data – General.* The primary clause used to define computer software license (not data/intellectual property first produced under this contractor or order) is FAR 52.227-19, *Commercial Computer Software License.*

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

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

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

and/or Government Accountability Office (GAO) staff during periodic control assessments, audits, or investigations.

e. The contractor may only use VA information within the terms of the contract and applicable Federal law, regulations, and VA policies. If new Federal information security laws, regulations

or VA policies become applicable after execution of the contract, the parties agree to negotiate contract modification and adjustment necessary to implement the new laws, regulations, and/or policies.

f. The contractor shall not make copies of VA information except as specifically authorized and necessary to 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 contactor.

h. The contractor shall store and transmit VA sensitive information in an encrypted form, using VA-approved encryption tools which are, at a minimum, Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules (or its successor) validated and in conformance 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.

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

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

o. Any media, such as paper, magnetic tape, magnetic disks, solid state devices or optical discs that 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.

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

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

(3) 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.

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

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

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

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

g. Contractors/subcontractors who no longer require VA 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.

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

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

b. The contractor shall provide 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: (1) The date and time (or approximation of) the Security Incident occurred.

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

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

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

(5) 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 employes shall fully cooperate with VA or third-party entity performing an independent risk analysis on behalf of VA. Failure to cooperate may be deemed a material breach and grounds for contract termination.

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

e. In instances of theft or break-in or other criminal activity, the contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG, and the VA Office of Security and Law Enforcement. The contractor, its employees, and its subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal 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.

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

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

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

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

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

b. Contracted new developments require creation, testing, evaluation, and authorization in compliance with VA Assessment and Authorization (A&A) processes in VA Handbook 6500 and VA Information Security Knowledge Service to obtain 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 though the COR/CO to identify the VA organization responsible for governance or resolution. Contractors shall comply with FAR 39.1, specifically the prohibitions referenced.

d. The contractor (including producers and resellers) shall comply with Office of Management and Budget (OMB) M-22-18 and M-23-16 when using third-party software on VA information systems or otherwise affecting the VA information. This includes new software purchases and software renewals for software developed or modified by major version change after the issuance date of M-22-18 (September 14, 2022). The term “software” includes firmware, operating systems, applications and application services (e.g., cloud-based software), as well as products containing software. The contractor shall provide a self-attestation that secure software development practices are utilized as outlined by Executive Order (EO)14028 and NIST Guidance. A third-party assessment provided by either a certified Federal Risk and Authorization Management Program (FedRAMP) Third Party Assessor Organization (3PAO) or one approved by the agency will be acceptable in lieu of a software producer's self-attestation.

e. The contractor shall ensure all delivered applications, systems and information systems are compliant with Homeland Security Presidential Directive (HSPD) 12 and VA Identity and Access management (IAM) enterprise identity management requirements as set forth in OMB M-19-17, M-05-24, FIPS 201-3,

Personal Identity Verification (PIV) of Federal Employees and Contractors (or its successor), M-21-31 and supporting NIST guidance. This applies to Commercial Off-The-Shelf (COTS) product(s) that the contractor did not develop, all software configurations and all customizations.

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

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

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

~~7. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE OR USE.~~

INTENTIONALLY DELETED ~~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.~~

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: (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.

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: (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.

13. **SPECIALIZED DEVICES/SYSTEMS (MEDICAL DEVICES, SPECIAL PURPOSE SYSTEMS, RESEARCH SCIENTIFIC COMPUTING).** This entire section applies when the acquisition includes one or more Medical Device, Special Purpose System or Research Scientific Computing Device. If appropriate, ensure selected clauses from section 6 or 7 and 8 through 12 are included. a. Contractor supplies/delivered Medical Devices, Special Purpose Systems-Operational Technology (SPS-OT) and Research Scientific Computing Devices shall comply with all applicable Federal law, regulations, and VA policies. New developments require creation, testing, evaluation, and authorization in compliance with processes specified on the Specialized Device Cybersecurity Department Enterprise Risk Management (SDCD-ERM) Portal, VA Directive 6550, *Pre-Procurement Assessment and Implementation of Medical Devices/Systems*, VA Handbook 6500, and the VA Information Security Knowledge Service. Deviations from Federal law, regulations, and VA Policy are identified and documented as part of VA Directive 6550 and/or the VA Enterprise Risk Analysis (ERA) processes for Specialized Devices/Systems processes.

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

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

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

(3) Due to the highly specialized and sometimes proprietary hardware and software associated with the device, if it is not possible for VA to retain the hard drive, firmware, and solid state, then: (a) The equipment contractor shall have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact.

(b) Any fixed hard drive, Complementary Metal-Oxide-Semiconductor (CMOS), Programmable Read-Only Memory (PROM), solid state and firmware on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be pre-approved and described in the solicitation, contract, or order.

~~14. **DATA CENTER PROVISIONS.** ***INTENTIONALLY DELETED*** 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.~~

B.3 RECORDS MANAGEMENT OBLIGATIONS

NARA Records Management Language for Contracts (July 10, 2019)

https://www.archives.gov/records-mgmt/policy/records-mgmt-language

RECORDS MANAGEMENT OBLIGATIONS

A. Applicability

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

B. Definitions

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

The term Federal record:

Includes [Agency] records.
Does not include personal materials.
Applies to records created, received, or maintained by Contractors pursuant to their [Agency] contract.
May include deliverables and documentation associated with deliverables.

C. Requirements

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

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

3. In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

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

5. The Contractor shall immediately notify the appropriate Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the [contract vehicle]. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to [Iowa City] control or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer

or address prescribed in the [contract vehicle]. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

6. The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any sub-contractor) is required to abide by Government and [Iowa City] guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.

7. The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with [Iowa City] policy.

8. The Contractor shall not create or maintain any records containing any non-public [Iowa City] information that are not specifically tied to or authorized by the contract.

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

10. The [Iowa City] owns the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which [Iowa City] shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.

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

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

D. Flow down of Requirements to Subcontractors

1. The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this [contract vehicle], and require written subcontractor acknowledgment of same.

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

B.4 PRICE/COST SCHEDULE

ITEM INFORMATION

ITEM NUMBER	DESCRIPTION OF SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	MR Patient Care Portal 5000 PRINCIPAL NAICS CODE: 339113 - Surgical Appliance and Supplies Manufacturing PRODUCT/SERVICE CODE: 6525 - Imaging Equipment and Supplies: Medical, Dental, Veterinary LOCAL STOCK NUMBER: 866162	2.00	EA	_____	_____
0002	Standard Accessories PRINCIPAL NAICS CODE: 339113 - Surgical Appliance and Supplies Manufacturing PRODUCT/SERVICE CODE: 6525 - Imaging Equipment and Supplies: Medical, Dental, Veterinary LOCAL STOCK NUMBER: 866162-A01	2.00	EA	_____	_____
0003	Patient Monitors PRINCIPAL NAICS CODE: 339113 - Surgical Appliance and Supplies Manufacturing PRODUCT/SERVICE CODE: 6525 - Imaging Equipment and Supplies: Medical, Dental, Veterinary LOCAL STOCK NUMBER: 866162-S01	2.00	EA	_____	_____
0004	Security & Remote Monitor PRINCIPAL NAICS CODE: 339113 - Surgical Appliance and Supplies Manufacturing PRODUCT/SERVICE CODE: 6525 - Imaging Equipment and Supplies: Medical, Dental, Veterinary LOCAL STOCK NUMBER: 866162-S02	2.00	EA	_____	_____
0005	Desktop Unit PRINCIPAL NAICS CODE: 339113 - Surgical Appliance and Supplies Manufacturing PRODUCT/SERVICE CODE: 6525 - Imaging Equipment and Supplies: Medical, Dental, Veterinary LOCAL STOCK NUMBER: 866162-H01	2.00	EA	_____	_____
0006		2.00	EA	_____	_____

	18.5 Inch Display PRINCIPAL NAICS CODE: 339113 - Surgical Appliance and Supplies Manufacturing PRODUCT/SERVICE CODE: 6525 - Imaging Equipment and Supplies: Medical, Dental, Veterinary LOCAL STOCK NUMBER: 866162-H02				
0007		2.00	EA	_____	_____
	Expression MR400 2.0 SW Update PRINCIPAL NAICS CODE: 339113 - Surgical Appliance and Supplies Manufacturing PRODUCT/SERVICE CODE: 6525 - Imaging Equipment and Supplies: Medical, Dental, Veterinary LOCAL STOCK NUMBER: 989803218881				
			GRAND TOTAL		_____

B.5 DELIVERY SCHEDULE

ITEM NUMBER	SHIPPING INFORMATION		QUANTITY	DELIVERY DATE
0001	SHIP TO:	Department of Veterans Affairs Iowa City VA Medical Center 601 Highway 6 West Iowa City, IA 52246 United States	2.00	
	MARK FOR:	Ryan Coapstick 319-338-0581 Ext. 5988 Ryan.Coapstick@va.gov		

SECTION C - CONTRACT CLAUSES

C.1 52.212-4 CONTRACT TERMS AND CONDITIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (OCT 2025) (DEVIATION)

(a) *Definitions*. The clause at Federal Acquisition Regulation (FAR) 52.202-1, Definitions, is incorporated by reference.

(b) *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.

(c) *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.

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

(e) *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 FAR 52.233-1, Disputes, which is incorporated in this contract by reference. The Contractor shall proceed diligently with performance of this contract, pending final resolution of any dispute arising under the contract.

(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. Examples of occurrences include 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. When an excusable delay occurs, the Contractor shall—

(1) Notify the Contracting Officer in writing as soon as possible;

(2) Remedy the delay as quickly as possible; and

(3) Notify the Contracting Officer when the occurrence is over.

(g) *Invoice.* The Government will handle invoices according to the Prompt Payment Act (31 U.S.C. 3903) and 5 CFR part 1315. The Contractor shall submit invoices to the address designated in the contract to receive invoices. An invoice must include the information required by 5 CFR part 1315.9(b).

(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) *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 that appears on the payment check or the specified payment date if an electronic funds transfer payment is made.

(4) *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;

(D) Contractor point of contact; and

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

(5) *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 FAR part 33 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 FAR part 32).

(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 termination for cause.

(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 for interest credits prescribed in FAR part 32 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 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. The Government will send a cure notice to the Contractor, unless the reason for the termination is late delivery. 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 under this contract 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) *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; 40 U.S.C. chapter 37, Contract Work Hours and Safety Standards; 41 U.S.C. chapter 87, Kickbacks; 49 U.S.C. 40118, Government-financed air transportation; and 41 U.S.C. chapter 21 relating to procurement integrity.

(r) *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 Disputes, Payments, Invoice, Compliance with Laws Unique to Government Contracts, and Unauthorized Obligations paragraphs of this clause;

(3) Other contract clauses incorporated in the solicitation or contract;

(4) Addenda to this solicitation or contract,

(5) Solicitation provisions incorporated in the solicitation.

(6) Other paragraphs of this clause.

(7) Other documents, exhibits, and attachments; and

(8) The specification.

(s) *Unauthorized obligations*.

(1) Except as stated in paragraph (s)(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 (s)(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.

(t) *Comptroller General examination of record*. This paragraph applies if this contract was awarded using other than sealed bid procedures and is in excess of the simplified acquisition threshold on the date of award of this contract.

(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 part 4, longer period

required by statute, or periods specified in 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 clause 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.

(u) *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 PRODUCTS AND COMMERCIAL SERVICES

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 52.222-36 EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES (NOV 2025) (DEVIATION)

(a) *Equal opportunity clause*. The Contractor must abide by the requirements of the equal opportunity clause at 41 CFR 60-741.5(a), as of March 24, 2014. This clause prohibits discrimination against qualified individuals on the basis of disability, and requires affirmative action by the Contractor to employ and advance in employment qualified individuals with disabilities.

(b) *Subcontracts*. The Contractor must include the terms of this clause in every subcontract or purchase order in excess of the threshold specified in Federal Acquisition Regulation (FAR) 22.1401-2(a)(1) on the date of subcontract award, unless exempted by rules, regulations, or orders of the Secretary, so that such provisions will be binding upon each subcontractor or vendor. The Contractor must act as specified by the Director, Office of Federal Contract Compliance Programs of the U.S. Department of Labor, to enforce the terms, including action for noncompliance. Such necessary changes in language may be made as shall be appropriate to identify properly the parties and their undertakings.

(End of Clause)

C.3 52.222-90 ADDRESSING DEI DISCRIMINATION BY FEDERAL CONTRACTORS (DEVIATION APR 2026)

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

Program participation means membership or participation in, or access or admission to: training, mentoring, or leadership development programs; educational opportunities; clubs; associations; or similar opportunities that are sponsored or established by the contractor or subcontractor.

Racially discriminatory diversity, equity, and inclusion (DEI) activities means disparate treatment based on race or ethnicity in the recruitment, employment (e.g., hiring, promotions), contracting (*e.g.*, vendor agreements), program participation, or allocation or deployment of an entity's resources.

(b) In connection with the performance of work under this contract, the Contractor agrees as follows:

(1) The Contractor will not engage in any racially discriminatory DEI activities;

(2) The Contractor will furnish all information and reports, including providing access to books, records, and accounts, as required by the Contracting Officer, for purposes of ascertaining compliance with this clause;

(3) In the event of the Contractor's or a subcontractor's noncompliance with this clause, this contract may be canceled, terminated, or suspended in whole or in part, and the Contractor or subcontractor may be declared ineligible for further Government contracts;

(4) The Contractor will report any subcontractor's known or reasonably knowable conduct that may violate this clause to the Contracting Officer and take any appropriate remedial actions directed by the Contracting Officer; and

(5) The Contractor will inform the Contracting Officer if a subcontractor sues the Contractor and the suit puts at issue, in any way, the validity of this clause.

(6) The Contractor recognizes that compliance with the requirements of this clause are material to the Government's payment decisions for purposes of 31 U.S.C. 3729(b)(4).

(c) The Contractor must include the substance of this clause, including this paragraph (c), in subcontracts at any tier, including those for commercial products and commercial services, except those where the place of delivery or performance is outside the United States.

(End of Clause)

C.4 52.223-23 SUSTAINABLE PRODUCTS (NOV 2025) (DEVIATION)

(a) Definitions. As used in this clause—

Sustainable products means—

(1) A product that contains recovered material designated by the EPA under the Comprehensive Procurement Guidelines (42 U.S.C. 6962) (40 CFR part 247) (*https://www.epa.gov/smm/comprehensive-procurement-guideline-cpg-program#products).*

(2) An energy-efficient product or low standby power device (42 U.S.C. 8259b) (10 CFR part 436, subpart C) (https://www.energy.gov/femp/search-energy-efficient-products,

https://www.energystar.gov/products?s=mega, and https://www.energy.gov/femp/low-standby-power-product-list).

(3) A biobased product that meets the content requirements of the USDA under the BioPreferred® program (7 U.S.C. 8102) (7 CFR Part 4270) (https://www.biopreferred.gov/)

(4) A substance identified in the EPA's Significant New Alternatives Policy (SNAP) program as a safe alternative to an ozone-depleting substance (42 U.S.C. 7671l) (40 CFR part 82, subpart G) (https://www.epa.gov/snap/unacceptable-and-acceptable-substitutes-tables).

(b) Requirements. The Government has identified in the statement of work or elsewhere in the contract the sustainable products that are required during the performance of this contract. The Contractor shall ensure that it provides sustainable products as required by this contract, when the products are—

(1) Delivered to the Government;

(2)Furnished for use by the Government;

(3) Incorporated into the construction of a public building or public work; or

(c) Furnished for use in performing services under this contract, where the cost of the products is a direct cost to this contract.

(End of Clause)

C.5 52.240-91 SECURITY PROHIBITIONS AND EXCLUSIONS (NOV 2025) (DEVIATION)

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

American Security Drone Act-covered foreign entity means an entity included on a list that the Federal Acquisition Security Council (FASC) develops and maintains and publishes in the System for Award Management (SAM) at *https://www.sam.gov* (section 1822 of Pub. L. 118-31, 41 U.S.C. 3901 note prec.).

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered application means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.

Covered article, as defined in 41 U.S.C. 4713(k), means:

(1) Information technology, as defined in 40 U.S.C. 11101, including cloud computing services of all types;

(2) Telecommunications equipment or telecommunications service, as those terms are defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

(3) The processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program (see 32 CFR part 2002); or

(4) Hardware, systems, devices, software, or services that include embedded or incidental information technology.

Covered foreign country means The People's Republic of China.

Covered telecommunications equipment or services means—

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means—

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled—

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

FASC-prohibited unmanned aircraft system means an unmanned aircraft system manufactured or assembled by an American Security Drone Act—covered foreign entity.

FASCSA order means any of the following orders issued under the Federal Acquisition Supply Chain Security Act (FASCSA) requiring removing covered articles from executive agency information systems or excluding one or more named sources or named covered articles from executive agency procurement actions, as described in 41 CFR 201-1.303(d) and (e):

(1) The Secretary of Homeland Security may issue FASCSA orders that apply to civilian agencies, to the extent not covered by paragraph (2) or (3) of this definition. This type of FASCSA order may be referred to as a Department of Homeland Security (DHS) FASCSA order.

(2) The Secretary of Defense may issue FASCSA orders that apply to the Department of Defense (DoD) and national security systems other than sensitive compartmented information systems. This type of FASCSA order may be referred to as a DoD FASCSA order.

(3) The Director of National Intelligence (DNI) may issue FASCSA orders that apply to the intelligence community and sensitive compartmented information systems, to the extent not covered by paragraph (2) of this definition. This type of FASCSA order may be referred to as a DNI FASCSA order.

Information technology, as defined in 40 U.S.C. 11101(6)—

(1) Means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use—

(i) Of that equipment; or

(ii) Of that equipment to a significant extent in the performance of a service or the furnishing of a product;

(2) Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but

(3) Does not include any equipment acquired by a Federal contractor incidental to a Federal contract.

Intelligence community, as defined by 50 U.S.C. 3003(4), means the following—

(1) The Office of the Director of National Intelligence;

(2) The Central Intelligence Agency;

(3) The National Security Agency;

(4) The Defense Intelligence Agency;

(5) The National Geospatial-Intelligence Agency;

(6) The National Reconnaissance Office;

(7) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs;

(8) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy;

(9) The Bureau of Intelligence and Research of the Department of State;

(10) The Office of Intelligence and Analysis of the Department of the Treasury;

(11) The Office of Intelligence and Analysis of the Department of Homeland Security; or

(12) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

Interconnection arrangement means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connecting a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Kaspersky Lab-covered article means any hardware, software, or service that—

(1) Is developed or provided by a Kaspersky Lab-covered entity;

(2) Includes any hardware, software, or service developed or provided in whole or in part by a Kaspersky Lab-covered entity; or

(3) Contains components using any hardware or software developed in whole or in part by a Kaspersky Lab-covered entity.

Kaspersky Lab-covered entity means—

(1) Kaspersky Lab;

(2) Any successor entity to Kaspersky Lab, including any change in name, e.g., "Kaspersky";

(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or

(4) Any entity of which Kaspersky Lab has a majority ownership.

National security system, as defined in 44 U.S.C. 3552, means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

(1) The function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or

(2) Is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Sensitive compartmented information means classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence.

Sensitive compartmented information system means a national security system authorized to process or store sensitive compartmented information.

Source means a non-Federal supplier, or potential supplier, of products or services, at any tier.

Subsidiary means an entity in which more than 50 percent of the entity is owned directly by a parent corporation or through another subsidiary of a parent corporation.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

Unmanned aircraft means an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft (49 U.S.C. 44801(11)).

Unmanned aircraft system means an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system (49 U.S.C. 44801(12)).

(b) *Prohibitions on providing or using specific products or services in performance of contract*. Unless a waiver or exception applies, the Contractor is prohibited from providing any products or services to the Government or using in the performance of the contract any of the following:

(1) A covered application on any information technology owned or managed by the Government, or on any information technology used or provided by the Contractor under this contract, including equipment provided by the Contractor’s employees (section 102 of Division R of the Consolidated Appropriations Act, 2023 (Pub. L. 117-328));

(2) A Kaspersky Lab-covered article (Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91));

(3) Covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system (paragraphs (a)(1)(A) of section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232)). This does not prohibit contractors from providing—

(i) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) Prohibition on unmanned aircraft systems manufactured or assembled by American Security Drone Act—covered foreign entities.

(1) Prohibition. The Contractor is prohibited from—

(i) Delivering any FASC-prohibited unmanned aircraft system, which includes unmanned aircraft (i.e., drones) and associated elements (sections 1823 and 1826 of American Security Drone Act of 2023, within the National Defense Authorization Act for Fiscal Year 2024, Pub. L. 118-31, Div. A, Title XVIII, Subtitle B, 41 U.S.C. 3901 note prec.);

(ii) On or after December 22, 2025, operating a FASC-prohibited unmanned aircraft system in the performance of the contract (section 1824 of Pub. L. 118-31); and

(iii) On or after December 22, 2025, using Federal funds to procure or operate a FASC-prohibited unmanned aircraft system (section 1825 of Pub. L. 118-31).

(2) *Procedures*. The Contractor shall search SAM for the FASC-maintained list of American Security Drone Act—covered foreign entities before proposing, or using in performance of the contract, any unmanned aircraft system. Also, the Contractor shall ensure any effort or expenditure associated with a FASC-prohibited unmanned aircraft system is consistent with a corresponding exemption, exception, or waiver determination expressly stated in the contract.

(3) *Exemptions, exceptions, and waivers*. The prohibitions in paragraph (c) of this clause do not apply where the agency has determined an exemption, exception, or waiver applies, and the contract indicates that such a determination has been made. See sections 1823 through 1825 and 1832 of Public Law 118-31 for statutory requirements pertaining to exemptions, exceptions, and waivers.

(d) *Prohibition on using or providing specific products or services or conducting certain transactions regardless of connection to contract*.

(1) *Certain telecommunications and video surveillance equipment, systems, or services*.

(i) Unless an applicable waiver has been issued by the Government, the Contractor cannot use any equipment, systems, or services that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part

of any system (paragraph (a)(1)(B) of section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232)).

(ii) This prohibition applies to using covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. This does not prohibit the contractor from using—

(A) A service that connects to the facilities of a third party, such as backhaul, roaming, or interconnection arrangements; or

(B) Telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(2) *Office of Foreign Assets Control Restrictions*.

(i) Except as authorized by the Office of Foreign Assets Control (OFAC) in the Department of the Treasury, the Contractor shall not acquire, for use in the performance of this contract, any supplies or services if any proclamation, Executive order, or statute administered by OFAC, or if OFAC's implementing regulations at 31 CFR chapter V, would prohibit such a transaction by a person subject to the jurisdiction of the United States.

(ii) Except as authorized by OFAC, most transactions involving Cuba, Iran, and Sudan are prohibited, as are most imports from Burma or North Korea, into the United States or its outlying areas.

(A) For lists of entities and individuals subject to economic sanctions, see OFAC's List of Specially Designated Nationals and Blocked Persons at *https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists*.

(B) For more information about these restrictions, as well as updates, see OFAC's regulations at 31 CFR chapter V and at *https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information*.

(C) To conduct electronic screens of potential parties to regulated transactions, see the consolidated screening list at *https://www.trade.gov/consolidated-screening-list*, which consolidates multiple export screening lists of the Departments of Commerce, State, and the Treasury.

(3) *Sudan prohibition*. The Contractor is prohibited from conducting any restricted business operations in Sudan in accordance with Accountability and Divestment Act of 2007 (Pub. L. 110-174).

(4) *Iran prohibitions*.

(i) Unless an exception applies according to paragraph (d)(4)(iii) or the Government grants a waiver, the contractor shall not engage in certain activities or transactions relating to Iran (section 6(b)(1)(A) of Iran Sanctions Act (50 U.S.C. 1701 note).

(ii) Unless an exception applies according to paragraph (d)(4)(iii) or the Government grants a waiver, contractor shall not export certain sensitive technology to Iran, as determined by the President, and has an active exclusion in SAM (22 U.S.C. 8515).

(iii) The prohibition in paragraphs (d)(4)(i) and (d)(4)(ii) do not apply if the acquisition is subject to trade agreements and the offeror certifies that all the offered products are designated country end products or designated country construction material (see part 25).

(iv) Unless an exception applies or the Government grants a waiver, contractors are prohibited from knowingly engaging in any significant transaction (i.e., over $15,000) with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked according to the International Emergency Economic Powers Act (section 6(b)(1)(B) of Iran Sanctions Act (50 U.S.C. 1701 note)).

(e) *Governmentwide exclusion and removal orders*.

(1) Unless the Government has issued an applicable waiver, contractors shall not provide or use as part of the performance of the contract any covered article, or any products or services produced or provided by a source, if the covered article or the source is prohibited by an applicable FASCSA order as follows:

(i) For solicitations and contracts awarded by a Department of Defense contracting office, DoD FASCSA orders apply.

(ii) For all other solicitations and contracts, DHS FASCSA orders apply.

(2) The Contractor shall search for the phrase "FASCSA order" in the System for Award Management (SAM) at *https://www.sam.gov* to locate applicable FASCSA orders.

(3) The Government may identify in the solicitation other FASCSA orders that are not in SAM, which are effective and apply to the solicitation and resulting contract.

(4) A FASCSA order issued after the date of solicitation applies to this contract only if added by an amendment to the solicitation or modification to the contract (see FAR 40.204-1(c)).

(f)*Reasonable inquiry*. The contractor shall conduct a reasonable inquiry to determine if there are any prohibited products or services. The inquiry will look at any information in the entity's possession but does not need to include an internal or third-party audit.

(g) *Removal of prohibited products and services*. For Federal Supply Schedules, Governmentwide acquisition contracts, multi-agency contracts or any other procurement instrument intended for use by multiple agencies, upon notification from the Contracting Officer, during the performance of the contract, the Contractor shall promptly make any necessary changes or modifications to remove any product or service produced or provided by a source that this clause prohibits.

(h) *General report*.

(1) If the Contractor identifies or is notified by any source, (including a subcontractor at any tier), that any product or service provided or used (or to be provided or used) during contract performance does not comply with any prohibition in this clause, then the Contractor shall report

the following information, or as much information is known, in writing to the contracting office as identified in paragraph (h)(2) within 72 hours:

(i) Contract number and order number, if applicable;

(ii) The specific prohibition the product or service is not complying with;

(iii) A description of the products or services that the Contractor identifies or has reason to suspect is prohibited (include brand; model number, such as the original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);

(iv) The entity that produced the product or service (include entity name, unique entity identifier, Contractor and Government Entity (CAGE) code, facilities responsible for design, fabrication, assembly, packaging, and test of the product, and whether the entity was the OEM or a distributor (provide manufacturer codes and distributor codes used for the product));

(v) Description of the functionality of the product or service and how that functionality impacts the risk to the product or service;

(vi) An explanation of any factors relevant to determining if the product or service should be permitted by an applicable exception, exemption, or waiver (if the contractor would like the Government to consider a waiver, and asks for such a waiver);

(vii) Whether alternative products or services are available that would comply with the prohibition;

(viii) If the product or service is related to item maintenance, include the following information on the item being maintained:

(A) Brand;

(B) Model number, OEM number, manufacturer part number, or wholesaler number; and

(C) Item description, as applicable.

(ix) Any readily available information about mitigation actions implemented or recommended.

(2) If a report must be submitted to a contracting office, the Contractor shall submit the report as follows:

(i) If a Department of Defense contracting office, the Contractor shall report to the website at *https://dibnet.dod.mil*.

(ii) For all other contracting offices, the Contractor shall report to the Contracting Officer.

(iii) For indefinite delivery contracts, the Contractor shall report to both the contracting office for the indefinite delivery contract and the contracting office for any affected order.

(3) If the report provided does not contain any of the information required by paragraph (h)(1) of this clause, and the contractor later discovers new information that is required by paragraph

(h)(1) of this clause, then the contractor shall submit a subsequent report within 72 hours of discovering the new information.

(4) The contractor shall also report the information in paragraph (h)(1) if the contractor wishes to ask for a waiver of the requirements of a new FASCSA order being applied through modification.

(i) *New FASCSA orders report*.

(1) During contract performance, the Contractor shall review SAM at least once every three months, or as advised by the Contracting Officer, to check for covered articles subject to FASCSA order(s), or for products or services produced by a source subject to FASCSA order(s) not currently identified under paragraph (e) of this clause.

(2) If the Contractor identifies a new FASCSA order(s) that could impact their supply chain, then the Contractor shall conduct a reasonable inquiry to identify whether a covered article or product or service produced or provided by a source subject to the FASCSA order(s) was provided to the Government or used during contract performance. The inquiry will look at any information in the entity's possession but does not need to include an internal or third-party audit.

(3) The Contractor shall submit a report to the contracting office identified in paragraph (h)(2) of this clause if the Contractor identifies, including through any notification by a subcontractor at any tier, that a covered article or product or service produced or provided by a source was provided to the Government or used during contract performance and is subject to a FASCSA order(s). For indefinite delivery contracts, the Contractor shall report to both the contracting office for the indefinite delivery contract and the contracting office for any affected order. The Contractor shall report the following information within 72 hours for each covered article or each product or service produced or provided by a source, where the covered article or source is subject to a FASCSA order:

(i) Contract number and order number, if applicable;

(ii) Name of the covered article or source subject to a FASCSA order;

(iii) The specific FASCSA order the product or service does not comply with;

(iv) The elements of (h)(1)(iii) through (ix) of this clause.

(j) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (j) but excluding subparagraphs (d)(1) and (i)(1), in all subcontracts and other contractual instruments, including subcontracts for acquiring commercial products or commercial services.

(End of Provision)

C.6 VAAR 852.219-73 VA NOTICE OF TOTAL SET-ASIDE FOR CERTIFIED SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESSES (JAN 2023) (DEVIATION)

(a) *Definition*. for the Department of Veterans Affairs, ‘‘*Service-disabled Veteran-owned small business concern or SDVOSB”*:

(1) Means a small business concern—

(i) Not less than 51 percent of which is owned by one or more service-disabled Veterans or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more service-disabled Veterans or eligible surviving spouses (see VAAR 802.201, Surviving Spouse definition);

(ii) The management and daily business operations of which are controlled by one or more service-disabled Veterans (or eligible surviving spouses) or, in the case of a service-disabled Veteran with permanent and severe disability, the spouse or permanent caregiver of such Veteran;

(iii) The business meets Federal small business size standards for the applicable North American Industry Classification System (NAICS) code identified in the solicitation document;

(iv) The business has been certified for ownership and control pursuant to 38 U.S.C. 8127, 13 CFR 128, and is listed as certified in the SBA certification database at *https://veterans.certify.sba.gov/*; and

(v) The business agrees to comply with VAAR subpart 819.70 and Small Business Administration (SBA) regulations regarding small business size, government contracting, and the Veteran Small Business Certification Program at 13 CFR parts 121, 125, and 128.

(2) The term ‘‘Service-disabled Veteran’’ means a Veteran, as defined in 38 U.S.C. 101(2), with a disability that is service-connected, as defined in 38 U.S.C. 101(16).

(3) The term ‘‘small business concern’’ has the meaning given that term under section 3 of the Small Business Act (15 U.S.C. 632).

(4) The term ‘‘small business concern owned and controlled by Veterans with service-connected disabilities’’ has the meaning given the term ‘‘*small business concern owned and controlled by service-disabled veterans*’’ under section 3(q)(2) of the Small Business Act (15 U.S.C. 632(q)(2)).

(5) The term *“SDVOSB participant”* or *certified SDVOSB* means a small business that has been certified in the SBA Veteran Small Business Certification Program and listed in the SBA certification database (see 13 CFR 128.102).

(b) *General*. In order for a concern to submit an offer and be eligible for the award of an SDVOSB set-aside or sole source contract, the concern must qualify as a small business concern under the size standard corresponding to the NAICS code assigned to the contract and be listed as an SDVOSB participant in the SBA certification database as set forth in 13 CFR 128.

(1) Offers received from entities that are not certified SDVOSBs and listed in the SBA certification database at the time of offer shall not be considered.

(2) Any award resulting from this solicitation shall be made to a certified SDVOSB listed in the SBA certification database who is eligible at the time of submission of offer(s) and at the time of award.

(3) The requirements in this clause apply to any contract, order or subcontract where the firm receives a benefit or preference from its designation as an SDVOSB, including set-asides, sole source awards, and evaluation preferences.

(c) *Representation*. Pursuant to 38 U.S.C. 8127(e), only certified SDVOSBs listed in the SBA certification database are considered eligible to receive award of a resulting contract. By submitting an offer, the prospective contractor represents that it is an eligible and certified SDVOSB as defined in this clause, 13 CFR 121, 125, and 128, and VAAR subpart 819.70.

(d) *Agreement/LOS certification.* When awarded a contract action, including orders under multipleaward contracts, an SDVOSB agrees that in the performance of the contract, the SDVOSB shall comply with requirements in VAAR subpart 819.70 and SBA regulations on small business size, and government contracting programs at 13 CFR part 121 and part 125, including the non-manufacturer rule and limitations on subcontracting (LOS) requirements in 13 CFR 121.406(b) and 13 CFR 125.6. For the purpose of limitations on subcontracting, only certified SDVOSBs listed in the SBA certification database (including independent contractors) shall be considered eligible and/or ‘‘similarly situated’’ (i.e., a firm that has the same small business program status as the prime contractor). An otherwise eligible firm further agrees to comply with the required LOS certification requirements in this solicitation (see 852.219–75 or 852.219–76 as applicable). These requirements are summarized as follows:

(1) *Services*. In the case of a contract for services (except construction), the SDVOSB prime contractor will not pay more than 50% of the amount paid by the government to the prime for contract performance to firms that are not certified SDVOSBs listed in the SBA certification database (excluding direct costs to the extent they are not the principal purpose of the acquisition and the SDVOSB/ VOSB does not provide the service, such as airline travel, cloud computing services, or mass media purchases). When a contract includes both services and supplies, the 50 percent limitation shall apply only to the service portion of the contract.

(2) *Supplies/products*.

(i) In the case of a contract for supplies or products (other than from a non-manufacturer of such supplies), the SDVOSB prime contractor will not pay more than 50% of the amount paid by the government to the prime for contract performance, excluding the cost of materials, to firms that are not certified SDVOSBs listed in the SBA certification database. When a contract includes both supply and services, the 50 percent limitation shall apply only to the supply portion of the contract.

(ii) In the case of a contract for supplies from a non-manufacturer, the SDVOSB prime contractor will supply the product of a domestic small business manufacturer or processor, unless a waiver as described in 13 CFR 121.406(b)(5) has been granted. Refer to 13 CFR 125.6(a)(2)(ii) for guidance pertaining to multiple item procurements.

(3) *General construction*. In the case of a contract for general construction, the SDVOSB prime contractor will not pay more than 85% of the amount paid by the government to the prime for contract performance, excluding the cost of materials, to firms that are not certified SDVOSBs listed in the SBA certification database.

(4) *Special trade construction contractors*. In the case of a contract for special trade contractors, no more than 75% of the amount paid by the government to the prime for contract performance, excluding the cost of materials, may be paid to firms that are not certified SDVOSBs listed in the SBA certification database.

(5) *Subcontracting*. An SDVOSB subcontractor must meet the NAICS size standard assigned by the prime contractor and be certified and listed in the SBA certification database to count as similarly situated. Any work that a first tier SDVOSB subcontractor further subcontracts will count towards the percent of subcontract amount that cannot be exceeded. For supply or construction contracts, the cost of materials is excluded and not considered to be subcontracted. When a contract includes both services and supplies, the 50 percent limitation shall apply only to the portion of the contract with the preponderance of the expenditure upon which the assigned NAICS is based. For information and more specific requirements, refer to 13 CFR 125.6.

(e) *Required limitations on subcontracting compliance measurement period*. An SDVOSB shall comply with the limitations on subcontracting as follows:

[X] By the end of the base term of the contract or order, and then by the end of each subsequent option period; or

[] By the end of the performance period for each order issued under the contract.

(f) *Joint ventures*. A joint venture may be considered eligible as an SDVOSB if the joint venture complies with the requirements in 13 CFR 128.402 and the managing joint venture partner makes the representations under paragraph (c) of this clause. A joint venture agrees that, in the performance of the contract, the applicable percentage specified in paragraph (d) of this clause will be performed by the aggregate of the joint venture participants.

(g) *Precedence*. The VA Veterans First Contracting Program, as defined in VAAR 802.101, subpart 819.70, and this clause, takes precedence over any inconsistencies between the requirements of the SBA Veteran Small Business Certification Program and the VA Veterans First Contracting Program.

(h) *Misrepresentation*. Pursuant to 38 U.S.C. 8127(g), any business concern, including all its principals, that is determined by VA to have willfully and intentionally misrepresented a company’s SDVOSB status is subject to debarment from contracting with the Department for a period of not less than five years (see VAAR 809.406–2 Causes for Debarment).

(End of Clause)

C.7 VAAR 852.219-76 VA NOTICE OF LIMITATIONS ON SUBCONTRACTING—CERTIFICATE OF COMPLIANCE FOR SUPPLIES AND PRODUCTS (JAN 2023) (DEVIATION)

(a) Pursuant to 38 U.S.C. 8127(l)(2), the offeror certifies that—

(1) If awarded a contract (see FAR 2.101 definition), it will comply with the limitations on subcontracting requirement as provided in the solicitation and the resultant contract, as follows:

(i) [ ] In the case of a contract for supplies or products (other than from a nonmanufacturer of such supplies), it will not pay more than 50% of the amount paid by the government to it to firms that are not certified SDVOSBs listed in the SBA certification database as set forth in 852.219–73 or certified VOSBs listed in the SBA certification database as set forth in 852.219–74. Any work that a similarly situated certified SDVOSB/VOSB subcontractor further subcontracts will count towards the 50% subcontract amount that cannot be exceeded. Cost of materials are excluded and not considered to be subcontracted.

(ii) [ ] In the case of a contract for supplies from a nonmanufacturer, it will supply the product of a domestic small business manufacturer or processor, unless a waiver as described in 13 CFR 121.406(b)(5) is granted. The offeror understands that, as provided in 13 CFR 121.406(b)(7), such a waiver has no effect on requirements external to the Small Business Act, such as the Buy American Act or the Trade Agreements Act.

(2) Manufacturer or nonmanufacturer representation and certification.

(i) [ ] *Manufacturer or producer*. The offeror certifies that it is the manufacturer or producer of the end item being procured, and the end item is manufactured or produced in the United States, in accordance with paragraph (a)(1)(i).

(ii) [ ] *Nonmanufacturer*. The offeror certifies that it qualifies as a nonmanufacturer in accordance with the requirements of 13 CFR 121.406(b) and paragraph (a)(1)(ii). The offeror further certifies it meets each element below as required in order to qualify as a nonmanufacturer.

[ ] The offeror certifies that it does not exceed 500 employees (or 150 employees for the Information Technology Value Added Reseller exception to NAICS code 541519, which is found at 13 CFR 121.201, footnote 18).

[ ] The offeror certifies that it is primarily engaged in the retail or wholesale trade and normally sells the type of item being supplied.

[ ] The offeror certifies that it will take ownership or possession of the item(s) with its personnel, equipment, or facilities in a manner consistent with industry practice.

(3) The offeror acknowledges that this certification concerns a matter within the jurisdiction of an Agency of the United States. The offeror further acknowledges that this certification is subject to Title 18, United States Code, Section 1001, and, as such, a false, fictitious, or fraudulent certification may render the offeror subject to criminal, civil, or administrative penalties, including prosecution.

(4) If VA determines that an SDVOSB/ VOSB awarded a contract pursuant to 38 U.S.C. 8127 did not act in good faith, such SDVOSB/VOSB shall be subject to any or all of the following:

(i) Referral to the VA Suspension and Debarment Committee;

(ii) A fine under section 16(g)(1) of the Small Business Act (15 U.S.C. 645(g)(1)); and

(iii) Prosecution for violating 18 U.S.C. 1001.

(b) The offeror represents and understands that by submission of its offer and award of a contract it may be required to provide copies of documents or records to VA that VA may review to determine whether the offeror complied with the limitations on subcontracting requirement specified in the contract or to determine whether the offeror qualifies as a manufacturer or nonmanufacturer in compliance with the limitations on subcontracting requirement. Contracting officers may, at their discretion, require the contractor to demonstrate its compliance with the limitations on subcontracting at any time during performance and upon completion of a contract if the information regarding such compliance is not already available to the contracting officer. Evidence of compliance includes, but is not limited to, invoices, copies of subcontracts, or a list of the value of tasks performed.

(c) The offeror further agrees to cooperate fully and make available any documents or records as may be required to enable VA to determine compliance. The offeror understands that failure to provide documents as requested by VA may result in remedial action as the Government deems appropriate.

(d) Offeror completed certification/fill-in required. The formal certification must be completed, signed and returned with the offeror’s bid, quotation, or proposal. The Government will not consider offers for award from offerors that do not provide the certification, and all such responses will be deemed ineligible for evaluation and award.

Certification

I hereby certify that if awarded the contract, _____ will comply with the limitations on subcontracting specified in this clause and in the resultant contract. I further certify that I am authorized to execute this certification on behalf of _____.

Printed Name of Signee: _____

Printed Title of Signee: _____

Signature: _____

Date: _____

Company Name and Address: _____

(End of Clause)

C.8 VAAR 852.247-73 PACKING FOR DOMESTIC SHIPMENT (OCT 2018)

Material shall be packed for shipment in such a manner that will insure acceptance by common carriers and safe delivery at destination. Containers and closures shall comply with regulations of carriers as applicable to the mode of transportation.

(End of Clause)

C.9 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):

https://www.acquisition.gov/browse/index/far
https://www.va.gov/oal/library/vaar/

(End of Clause)

FAR Number	Title	Date
52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS	NOV 2023
52.203-19	PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS	JAN 2017
52.204-13	SYSTEM FOR AWARD MANAGEMENT—MAINTENANCE (DEVIATION)	NOV 2025
52.209-10	PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS	NOV 2015
52.219-33	NONMANUFACTURER RULE (DEVIATION)	NOV 2025
52.222-19	CHILD LABOR—COOPERATION WITH AUTHORITIES AND REMEDIES (DEVIATION)	MAR 2026
52.222-50	COMBATING TRAFFICKING IN PERSONS (DEVIATION)	NOV 2025
52.226-8	ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING	MAY 2024
52.229-12	TAX ON CERTAIN FOREIGN PROCUREMENTS	FEB 2021
52.232-33	PAYMENT BY ELECTRONIC FUNDS TRANSFER—SYSTEM FOR AWARD MANAGEMENT	OCT 2018
52.232-40	PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS	MAR 2023
52.233-3	PROTEST AFTER AWARD	AUG 1996
52.233-4	APPLICABLE LAW FOR BREACH OF CONTRACT CLAIM	OCT 2004
52.247-64	PREFERENCE FOR PRIVATELY OWNED U.S.-FLAG COMMERCIAL VESSELS (DEVIATION) ALTERNATE I (APR 2003)	NOV 2025
852.203-70	COMMERCIAL ADVERTISING	MAY 2018
852.232-72	ELECTRONIC SUBMISSION OF PAYMENT REQUESTS	NOV 2018
852.242-71	ADMINISTRATIVE CONTRACTING OFFICER	OCT 2020
852.246-71	REJECTED GOODS	OCT 2018

(End of Addendum to 52.212-4)

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):
https://www.acquisition.gov/browse/index/far
https://www.va.gov/oal/library/vaar/

(End of Clause)

FAR Number	Title	Date
52.203-13	CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT	NOV 2021
52.203-16	PREVENTING PERSONAL CONFLICTS OF INTEREST	JUN 2020
52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS	NOV 2023
52.204-13	SYSTEM FOR AWARD MANAGEMENT MAINTENANCE	OCT 2018
52.204-27	PROHIBITION ON A BYTEDANCE COVERED APPLICATION	JUN 2023
52.204-29	FEDERAL ACQUISITION SUPPLY CHAIN SECURITY ACT ORDERS—REPRESENTATION AND DISCLOSURES	DEC 2023
52.209-10	PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS	NOV 2015
52.222-3	CONVICT LABOR	JUN 2003
52.222-35	EQUAL OPPORTUNITY FOR VETERANS	JUN 2020
52.222-37	EMPLOYMENT REPORTS ON VETERANS	JUN 2020
52.222-38	COMPLIANCE WITH VETERANS' EMPLOYMENT REPORTING REQUIREMENTS	FEB 2016
52.222-40	NOTIFICATION OF EMPLOYEE RIGHTS UNDER THE NATIONAL LABOR RELATIONS ACT	DEC 2010
52.222-41	SERVICE CONTRACT LABOR STANDARDS	AUG 2018
52.222-50	COMBATING TRAFFICKING IN PERSONS	OCT 2025
52.222-54	EMPLOYMENT ELIGIBILITY VERIFICATION	JAN 2025
52.222-62	PAID SICK LEAVE UNDER EXECUTIVE ORDER 13706	JAN 2022
52.226-8	ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING	MAY 2024
52.232-33	PAYMENT BY ELECTRONIC FUNDS TRANSFER—SYSTEM FOR AWARD MANAGEMENT	OCT 2018
52.233-1	DISPUTES	MAY 2014
52.233-3	PROTEST AFTER AWARD	AUG 1996
52.233-4	APPLICABLE LAW FOR BREACH OF CONTRACT CLAIM	OCT 2004
852.222-71	COMPLIANCE WITH EXECUTIVE ORDER 13899 (DEVIATION) (APR 2025)	APR 2025

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS

SECTION E - SOLICITATION PROVISIONS

E.1 52.212-1 INSTRUCTIONS TO OFFERORS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (OCT 2025) (DEVIATION)

(a) *Submission of offers*. Submit signed and dated offers to the office specified in this solicitation at or before the exact time specified in this solicitation. As a minimum, offers shall include—

(1) The solicitation number;

(2) The name, address, telephone number of the Offeror;

(3) The Offeror's Unique Entity Identifier (UEI) and, if applicable, Electronic Funds Transfer (EFT) indicator;

(4) Information necessary to evaluate the factors contained in the provision at 52.212-2 or as described in the solicitation;

(5) Responses to provisions that require Offeror completion of information, representations, and certifications (other than those collected via the System for Award Management (SAM)); and

(6) A statement specifying the extent of agreement with all terms, conditions, and provisions included in the solicitation and any solicitation amendments.

(b) *Period for acceptance of offers*. The Offeror agrees to hold the prices in its offer firm for 60 calendar days from the date specified for receipt of offers, unless another time period is specified in an addendum to the solicitation.

(c) *Late submissions, modifications, revisions, and withdrawals of offers*.

(1) Offerors are responsible for submitting offers and any modifications or revisions to the Government office designated in the solicitation by the time specified in the solicitation.

(2) Any offer, modification, or revision received after the time specified for receipt of offers is "late" and will not be considered unless it is received before award is made and the Contracting Officer determines that accepting the late offer would not unduly delay the acquisition. However, a late modification of an otherwise successful offer that makes its terms more favorable to the Government will be considered at any time it is received and may be accepted.

(3) If an emergency or unanticipated event interrupts normal Government processes so that offers cannot be received at the Government office designated for receipt of offers by the exact time specified in the solicitation, and urgent Government requirements preclude amendment of the solicitation or other notice of an extension of the closing date, the time specified for receipt of offers will be deemed to be extended to the same time of day specified in the solicitation on the first work day on which normal Government processes resume.

(4) Offerors may withdraw their offers by written notice to the Government received at any time before award.

(d) *Contract award (not applicable to Invitation for Bids)*. The Government intends to evaluate offers and award a contract without discussions with Offerors. Therefore, the Offeror's initial offer should contain the Offeror's best terms. However, the Government reserves the right to conduct discussions, if necessary. The Government may reject any or all offers if such action is in the public interest, accept other than the lowest offer, and waive informalities and minor irregularities in offers received.

(e) *Debriefings*. If a postaward debriefing is given to requesting Offerors, the Government will disclose the following information, if applicable:

(1) The agency's evaluation of the significant weak or deficient factors in the debriefed Offeror's offer.

(2) The overall evaluated cost or price and technical rating of the successful Offeror and the debriefed Offeror and past performance information on the debriefed Offeror.

(3) The overall ranking of all Offerors when any ranking was developed by the agency during source selection.

(4) A summary of the rationale for award.

(5) For acquisitions of commercial products, the make and model of the product to be delivered by the successful Offeror.

(6) Reasonable responses to relevant questions posed by the debriefed Offeror as to whether the agency followed source-selection procedures set forth in the solicitation, applicable regulations, and other applicable authorities.

(End of Provision)

ADDENDUM to FAR 52.212-1 INSTRUCTIONS TO OFFERORS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Provisions 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 provisions are incorporated into 52.212-1 as an addendum to this solicitation:

E.2 52.216-1 TYPE OF CONTRACT (NOV 2025) (DEVIATION)

The Government contemplates award of a Firm-Fixed-Price contract resulting from this solicitation.

(End of Provision)

E.3 52.225-1 BUY AMERICAN—SUPPLIES (NOV 2025) (DEVIATION)

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

Commercially available off-the-shelf (COTS) item—

(1) Means any item of supply (including construction material) that is–

(i) A commercial product (as defined in paragraph (1) of the definition of ‘‘commercial product’’ at Federal Acquisition Regulation (FAR) 2.101);

(ii) Sold in substantial quantities in the commercial marketplace; and

(iii) Offered to the Government, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace; and

(2) Does not include bulk cargo, as defined in 46 U.S.C. 40102(4), such as agricultural products and petroleum products.

Component means an article, material, or supply incorporated directly into an end product.

Cost of components means—

(1) For components purchased by the Contractor, the acquisition cost, including transportation costs to the place of incorporation into the end product (whether or not such costs are paid to a domestic firm), and any applicable duty (whether or not a duty-free entry certificate is issued); or

(2) For components manufactured by the Contractor, all costs associated with the manufacture of the component, including transportation costs as described in paragraph (1) of this definition, plus allocable overhead costs, but excluding profit. Cost of components does not include any costs associated with the manufacture of the end product.

Critical component means a component that is mined, produced, or manufactured in the United States and deemed critical to the U.S. supply chain. The list of critical components is at FAR 25.105.

Domestic end product means—

(1) For an end product that does not consist wholly or predominantly of iron or steel or a combination of both—

(i) An unmanufactured end product mined or produced in the United States;

(ii) An end product manufactured in the United States, if-

(A) The cost of its components mined, produced, or manufactured in the United States exceeds 60 percent of the cost of all its components, except that the percentage will be 65 percent for items delivered in calendar years 2024 through 2028 and 75 percent for items delivered starting in calendar year 2029. Components of foreign origin of the same class or kind as those that the agency determines are not mined, produced, or manufactured in sufficient and reasonably available commercial quantities of a satisfactory quality are treated as domestic. Components of unknown origin are treated as foreign. Scrap generated, collected, and prepared for processing in the United States is considered domestic; or

(B) The end product is a COTS item; or

(2) For an end product that consists wholly or predominantly of iron or steel or a combination of both, an end product manufactured in the United States, if the cost of foreign iron and steel constitutes less than 5 percent of the cost of all the components used in the end product. The cost of foreign iron and steel includes but is not limited to the cost of foreign iron or steel mill products (such as bar, billet, slab, wire, plate, or sheet), castings, or forgings utilized in the manufacture of the end product and a good faith estimate of the cost of all foreign iron or steel components excluding COTS fasteners. Iron or steel components of unknown origin are treated as foreign. If the end product contains multiple components, the cost of all the materials used in such end product is calculated in accordance with the definition of ‘‘cost of components’’.

End product means those articles, materials, and supplies to be acquired under the contract for public use.

Fastener means a hardware device that mechanically joins or affixes two or more objects together. Examples of fasteners are nuts, bolts, pins, rivets, nails, clips, and screws.

Foreign end product means an end product other than a domestic end product.

Foreign iron and steel means iron or steel products not produced in the United States. Produced in the United States means that all manufacturing processes of the iron or steel must take place in the United States, from the initial melting stage through the application of coatings, except metallurgical processes involving refinement of steel additives. The origin of the elements of the iron or steel is not relevant to the determination of whether it is domestic or foreign.

Predominantly of iron or steel or a combination of both means that the cost of the iron and steel content exceeds 50 percent of the total cost of all its components. The cost of iron and steel is the cost of the iron or steel mill products (such as bar, billet, slab, wire, plate, or sheet), castings, or forgings utilized in the manufacture of the product and a good faith estimate of the cost of iron or steel components excluding COTS fasteners.

Steel means an alloy that includes at least 50 percent iron, between 0.02 and 2 percent carbon, and may include other elements.

United States means the 50 States, the District of Columbia, and outlying areas.

(b) 41 U.S.C. chapter 83, Buy American, provides a preference for domestic end products for supplies acquired for use in the United States. In accordance with 41 U.S.C. 1907, the domestic content test of the Buy American statute is waived for an end product that is a COTS item, except that for an end product that consists wholly or predominantly of iron or steel or a combination of both, the domestic content test is applied only to the iron and steel content of the end product, excluding COTS fasteners.

(c) Offerors may obtain from the Contracting Officer a list of foreign articles that the Contracting Officer will treat as domestic for this contract.

(d) The Contractor shall deliver only domestic end products except to the extent that it specified delivery of foreign end products in the provision of the solicitation entitled "Buy American Certificate."

(End of Clause)

FAR Number	Title	Date
52.225-2	BUY AMERICAN CERTIFICATE	OCT 2022

E.4 52.225-3 BUY AMERICAN—FREE TRADE AGREEMENTS—ISRAELI TRADE ACT (DEVIATION) (NOV 2025) ALTERNATE III (DEVIATION) (NOV 2025)

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

Korean end product means an article that—

(1) Is wholly the growth, product, or manufacture of Korea (Republic of); or

(2) In the case of an article that consists in whole or in part of materials from another country, has been substantially transformed in Korea (Republic of) into a new and different article of commerce with a name, character, or use distinct from that of the article or articles from which it was transformed. The term refers to a product offered for purchase under a supply contract, but for purposes of calculating the value of the end product includes services (except transportation services) incidental to the article, provided that the value of those incidental services does not exceed that of the article itself.

Commercially available off-the-shelf (COTS) item—

(1) Means any item of supply (including construction material) that is-

(i) A commercial product (as defined in paragraph (1) of the definition of ‘‘commercial product’’ at Federal Acquisition Regulation (FAR) 2.101);

(ii) Sold in substantial quantities in the commercial marketplace; and

(iii) Offered to the Government, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace; and

(2) Does not include bulk cargo, as defined in 46 U.S.C. 40102(4), such as agricultural products and petroleum products.

Component means an article, material, or supply incorporated directly into an end product.

Cost of components means—

(1) For components purchased by the Contractor, the acquisition cost, including transportation costs to the place of incorporation into the end product (whether or not such costs are paid to a domestic firm), and any applicable duty (whether or not a duty-free entry certificate is issued); or

(2) For components manufactured by the Contractor, all costs associated with the manufacture of the component, including transportation costs as described in paragraph (1) of this definition, plus allocable overhead costs, but excluding profit. Cost of components does not include any costs associated with the manufacture of the end product.

Critical component means a component that is mined, produced, or manufactured in the United States and deemed critical to the U.S. supply chain. The list of critical components is at FAR 25.105.

Domestic end product means—

(1) For an end product that does not consist wholly or predominantly of iron or steel or a combination of both—

(i) An unmanufactured end product mined or produced in the United States;

(ii) An end product manufactured in the United States, if—

(A) The cost of its components mined, produced, or manufactured in the United States exceeds 60 percent of the cost of all its components, except that the percentage will be 65 percent for items delivered in calendar years 2024 through 2028 and 75 percent for items delivered starting in calendar year 2029. Components of foreign origin of the same class or kind as those that the agency determines are not mined, produced, or manufactured in sufficient and reasonably available commercial quantities of a satisfactory quality are treated as domestic. Components of unknown origin are treated as foreign. Scrap generated, collected, and prepared for processing in the United States is considered domestic; or

(B) The end product is a COTS item; or

(2) For an end product that consists wholly or predominantly of iron or steel or a combination of both, an end product manufactured in the United States, if the cost of foreign iron and steel constitutes less than 5 percent of the cost of all the components used in the end product. The cost of foreign iron and steel includes but is not limited to the cost of foreign iron or steel mill products (such as bar, billet, slab, wire, plate, or sheet), castings, or forgings utilized in the manufacture of the end product and a good faith estimate of the cost of all foreign iron or steel components excluding COTS fasteners. Iron or steel components of unknown origin are treated as foreign. If the end product contains multiple components, the cost of all the materials used in such end product is calculated in accordance with the definition of ‘‘cost of components’’.

End product means those articles, materials, and supplies to be acquired under the contract for public use.

Fastener means a hardware device that mechanically joins or affixes two or more objects together. Examples of fasteners are nuts, bolts, pins, rivets, nails, clips, and screws.

Foreign end product means an end product other than a domestic end product.

Foreign iron and steel means iron or steel products not produced in the United States. Produced in the United States means that all manufacturing processes of the iron or steel must take place in the United States, from the initial melting stage through the application of coatings, except metallurgical processes involving refinement of steel additives. The origin of the elements of the iron or steel is not relevant to the determination of whether it is domestic or foreign.

Free Trade Agreement country means Australia, Bahrain, Chile, Colombia, Costa Rica, Dominican Republic, El Salvador, Guatemala, Honduras, Korea (Republic of), Mexico, Morocco, Nicaragua, Oman, Panama, Peru, or Singapore.

Free Trade Agreement country end product means an article that-

(1) Is wholly the growth, product, or manufacture of a Free Trade Agreement country; or

(2) In the case of an article that consists in whole or in part of materials from another country, has been substantially transformed in a Free Trade Agreement country into a new and different article of commerce with a name, character, or use distinct from that of the article or articles from which it was transformed. The term refers to a product offered for purchase under a supply contract, but for purposes of calculating the value of the end product includes services (except transportation services) incidental to the article, provided that the value of those incidental services does not exceed that of the article itself.

Israeli end product means an article that—

(1) Is wholly the growth, product, or manufacture of Israel; or

(2) In the case of an article that consists in whole or in part of materials from another country, has been substantially transformed in Israel into a new and different article of commerce with a name, character, or use distinct from that of the article or articles from which it was transformed.

Predominantly of iron or steel or a combination of both means that the cost of the iron and steel content exceeds 50 percent of the total cost of all its components. The cost of iron and steel is the cost of the iron or steel mill products (such as bar, billet, slab, wire, plate, or sheet), castings, or forgings utilized in the manufacture of the product and a good faith estimate of the cost of iron or steel components excluding COTS fasteners.

Steel means an alloy that includes at least 50 percent iron, between 0.02 and 2 percent carbon, and may include other elements.

United States means the 50 States, the District of Columbia, and outlying areas.

(b) *Components of foreign origin*. Offerors may obtain from the Contracting Officer a list of foreign articles that the Contracting Officer will treat as domestic for this contract.

(c) *Delivery of end products.* 41 U.S.C. chapter 83 provides a preference for domestic end products for supplies acquired for use in the United States. In accordance with 41 U.S.C. 1907, the domestic content test of the Buy American statute is waived for an end product that is a COTS item, except that for an end product that consists wholly or predominantly of iron or steel or a combination of both, the domestic content test is applied only to the iron and steel content of the end product, excluding COTS fasteners. In addition, the Contracting Officer has determined that the Korea (Republic of) FTA and the Israeli Trade Act apply to this acquisition. Unless otherwise specified, these trade agreements apply to all items in the Schedule. The Contractor shall deliver under this contract only domestic end products except to the extent that, in its offer, it specified delivery of foreign end products in the provision entitled “Buy American—Free Trade Agreements—Israeli Trade Act Certificate.” If the Contractor specified in its offer that the Contractor would supply a Korean end product or an Israeli end product, then the Contractor

shall supply a Korean end product, an Israeli end product, or at the Contractor's option, a domestic end product.

(End of Clause)

E.5 52.225-4 BUY AMERICAN—FREE TRADE AGREEMENTS—ISRAELI TRADE ACT CERTIFICATE (DEVIATION) (NOV 2025) ALTERNATE II (JAN 2025)

(a)(1) The Offeror certifies that each end product, except those listed in paragraph (b) or (c)(1) of this provision, is a domestic end product and that each domestic end product listed in paragraph (c)(2) of this provision contains a critical component.

(2) The terms ''Bahraini, Moroccan, Omani, Panamanian, or Peruvian end product,'' ''commercially available off-the-shelf (COTS) item,'' ''critical component,'' ''domestic end product,'' ''end product,'' ''foreign end product,'' ''Free Trade Agreement country,'' ''Free Trade Agreement country end product,'' ''Israeli end product,'' and ''United States'' are defined in the clause of this solicitation entitled ''Buy American-Free Trade Agreements-Israeli Trade Act.''

(b) The offeror certifies that the following supplies are Israeli end products as defined in the clause of this solicitation entitled "Buy American-Free Trade Agreements-Israeli Trade Act".

Israeli End Products:

Line item No.

(c)(1) The Offeror shall list those supplies that are foreign end products (other than those listed in paragraph (b) of this provision) as defined in the clause of this solicitation entitled ''Buy American-Free Trade Agreements-Israeli Trade Act.''

Other Foreign End Products:

Line item No.	Country of origin

(2) The Offeror shall list the line item numbers of domestic end products that contain a critical component (see FAR 25.105).

Line Item No. _____

(d) The Government will evaluate offers in accordance with the policies and procedures of part 25 of the Federal Acquisition Regulation.

(End of Provision)

E.6 52.225-5 TRADE AGREEMENTS (NOV 2023)

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

"Caribbean Basin country end product"—

(1) Means an article that—

(i)(A) Is wholly the growth, product, or manufacture of a Caribbean Basin country; or

(B) In the case of an article that consists in whole or in part of materials from another country, has been substantially transformed in a Caribbean Basin country into a new and different article of commerce with a name, character, or use distinct from that of the article or articles from which it was transformed; and

(ii) Is not excluded from duty-free treatment for Caribbean countries under 19 U.S.C. 2703(b).

(A) For this reason, the following articles are not Caribbean Basin country end products:

(1) Tuna, prepared or preserved in any manner in airtight containers;

(2) Petroleum, or any product derived from petroleum;

(3) Watches and watch parts (including cases, bracelets, and straps) of whatever type including, but not limited to, mechanical, quartz digital, or quartz analog, if such watches or watch parts contain any material that is the product of any country to which the Harmonized Tariff Schedule of the United States (HTSUS) column 2 rates of duty apply (i.e., Afghanistan, Cuba, Laos, North Korea, and Vietnam); and

(4) Certain of the following: textiles and apparel articles; footwear, handbags, luggage, flat goods, work gloves, and leather wearing apparel; or handloomed, handmade, and folklore articles;

(B) Access to the HTSUS to determine duty-free status of articles of these types is available at *https://www.usitc.gov/tata/hts/index.htm*. In particular, see the following:

(1) General Note 3(c), Products Eligible for Special Tariff treatment.

(2) General Note 17, Products of Countries Designated as Beneficiary Countries under the United States—Caribbean Basin Trade Partnership Act of 2000.

(3) Section XXII, Chapter 98, Subchapter II, Articles Exported and Returned, Advanced or Improved Abroad, U.S. Note 7(b).

(4) Section XXII, Chapter 98, Subchapter XX, Goods Eligible for Special Tariff Benefits under the United States—Caribbean Basin Trade Partnership Act; and

(2) Refers to a product offered for purchase under a supply contract, but for purposes of calculating the value of the acquisition, includes services (except transportation services) incidental to the article, provided that the value of those incidental services does not exceed that of the article itself.

"Designated country" means any of the following countries:

(1) A World Trade Organization Government Procurement Agreement (WTO GPA) country (Armenia, Aruba, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea (Republic of), Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, New Zealand, North Macedonia, Norway, Poland, Portugal, Romania, Singapore, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Taiwan (known in the World Trade Organization as "the Separate Customs Territory of Taiwan, Penghu, Kinmen and Matsu (Chinese Taipei)"), Ukraine, or United Kingdom);

(2) A Free Trade Agreement (FTA) country (Australia, Bahrain, Chile, Colombia, Costa Rica, Dominican Republic, El Salvador, Guatemala, Honduras, Korea (Republic of), Mexico, Morocco, Nicaragua, Oman, Panama, Peru, or Singapore);

(3) A least developed country (Afghanistan, Angola, Bangladesh, Benin, Bhutan, Burkina Faso, Burundi, Cambodia, Central African Republic, Chad, Comoros, Democratic Republic of Congo, Djibouti, Equatorial Guinea, Eritrea, Ethiopia, Gambia, Guinea, Guinea-Bissau, Haiti, Kiribati, Laos, Lesotho, Liberia, Madagascar, Malawi, Mali, Mauritania, Mozambique, Nepal, Niger, Rwanda, Samoa, Sao Tome and Principe, Senegal, Sierra Leone, Solomon Islands, Somalia, South Sudan, Tanzania, Timor-Leste, Togo, Tuvalu, Uganda, Vanuatu, Yemen, or Zambia); or

(4) A Caribbean Basin country (Antigua and Barbuda, Aruba, Bahamas, Barbados, Belize, Bonaire, British Virgin Islands, Curacao, Dominica, Grenada, Guyana, Haiti, Jamaica, Montserrat, Saba, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Sint Eustatius, Sint Maarten, or Trinidad and Tobago).

"Designated country end product" means a WTO GPA country end product, an FTA country end product, a least developed country end product, or a Caribbean Basin country end product.

"End product" means those articles, materials, and supplies to be acquired under the contract for public use.

"Free Trade Agreement country end product" means an article that—

(1) Is wholly the growth, product, or manufacture of a Free Trade Agreement (FTA) country; or

(2) In the case of an article that consists in whole or in part of materials from another country, has been substantially transformed in an FTA country into a new and different article of commerce with a name, character, or use distinct from that of the article or articles from which it was transformed. The term refers to a product offered for purchase under a supply contract, but for purposes of calculating the value of the end product includes services, (except transportation services) incidental to the article, provided that the value of those incidental services does not exceed that of the article itself.

"Least developed country end product" means an article that—

(1) Is wholly the growth, product, or manufacture of a least developed country; or

(2) In the case of an article that consists in whole or in part of materials from another country, has been substantially transformed in a least developed country into a new and different article of commerce with a name, character, or use distinct from that of the article or articles from which it was transformed. The term refers to a product offered for purchase under a supply contract, but for purposes of calculating the value of the end product, includes services (except transportation services) incidental to the article, provided that the value of those incidental services does not exceed that of the article itself.

"United States" means the 50 States, the District of Columbia, and outlying areas.

"U.S.-made end product" means an article that is mined, produced, or manufactured in the United States or that is substantially transformed in the United States into a new and different article of commerce with a name, character, or use distinct from that of the article or articles from which it was transformed.

"WTO GPA country end product" means an article that—

(1) Is wholly the growth, product, or manufacture of a WTO GPA country; or

(2) In the case of an article that consists in whole or in part of materials from another country, has been substantially transformed in a WTO GPA country into a new and different article of commerce with a name, character, or use distinct from that of the article or articles from which it was transformed. The term refers to a product offered for purchase under a supply contract, but for purposes of calculating the value of the end product includes services, (except transportation services) incidental to the article, provided that the value of those incidental services does not exceed that of the article itself.

(b) *Delivery of end products.* The Contracting Officer has determined that the WTO GPA and FTAs apply to this acquisition. Unless otherwise specified, these trade agreements apply to all items in the Schedule. The Contractor shall deliver under this contract only U.S.-made or designated country end products except to the extent that, in its offer, it specified delivery of other end products in the provision entitled "Trade Agreements Certificate."

(End of Clause)

E.7 52.225-6 TRADE AGREEMENTS CERTIFICATE (FEB 2021)

(a) The offeror certifies that each end product, except those listed in paragraph (b) of this provision, is a U.S.-made or designated country end product, as defined in the clause of this solicitation entitled "Trade Agreements."

(b) The offeror shall list as other end products those supplies that are not U.S.-made or designated country end products.

Other End Products

Line item No.	Country of origin

[List as necessary]

(c) The Government will evaluate offers in accordance with the policies and procedures of Part 25 of the Federal Acquisition Regulation. For line items covered by the WTO GPA, the Government will evaluate offers of U.S.-made or designated country end products without regard to the restrictions of the Buy American statute. The Government will consider for award only offers of U.S.-made or designated country end products unless the Contracting Officer determines that there are no offers for such products or that the offers for those products are insufficient to fulfill the requirements of this solicitation.

(End of Provision)

E.8 52.240-90 SECURITY PROHIBITIONS AND EXCLUSIONS REPRESENTATIONS AND CERTIFICATIONS (NOV 2025) (DEVIATION)

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

Backhaul, covered article, covered telecommunications equipment or services, critical technology, FASCSA order, Intelligence community, interconnection arrangements, national security system, roaming, sensitive compartmented information, sensitive compartmented information system, source, and substantial or essential component have the meanings provided in the clause 52.240-91, Security Prohibitions and Exclusions.

Business operations means engaging in commerce in any form, including by acquiring, developing, maintaining, owning, selling, possessing, leasing, or operating equipment, facilities, personnel, products, services, personal property, real property, or any other apparatus of business or commerce.

Marginalized populations of Sudan means—

(1) Adversely affected groups in regions authorized to receive assistance under section 8(c) of the Darfur Peace and Accountability Act (Pub. L. 109-344) (50 U.S.C. 1701 note); and

(2) Marginalized areas in Northern Sudan described in section 4(9) of such Act.

Restricted business operations means business operations in Sudan that include power production activities, mineral extraction activities, oil-related activities, or the production of military equipment, as those terms are defined in the Sudan Accountability and Divestment Act of 2007 (Pub. L. 110-174). Restricted business operations do not include business operations that the person (as that term is defined in Section 2 of the Sudan Accountability and Divestment Act of 2007) conducting the business can demonstrate—

(1) Are conducted under contract directly and exclusively with the regional government of southern Sudan;

(2) Are conducted under specific authorization from the Office of Foreign Assets Control in the Department of the Treasury, or are expressly exempted under Federal law from the requirement to be conducted under such authorization;

(3) Consist of providing goods or services to marginalized populations of Sudan;

(4) Consist of providing goods or services to an internationally recognized peacekeeping force or humanitarian organization;

(5) Consist of providing goods or services that are used only to promote health or education; or

(6) Have been voluntarily suspended.

Sensitive technology—

(1) Means hardware, software, telecommunications equipment, or any other technology that is to be used specifically—

(i) To restrict the free flow of unbiased information in Iran; or

(ii) To disrupt, monitor, or otherwise restrict speech of the people of Iran; and

(2) Does not include information or informational materials the export of which the President does not have the authority to regulate or prohibit pursuant to section 203(b)(3) of the International Emergency Economic Powers Act (50 U.S.C. 1702(b)(3)).

(b) *Procedures*.

(1) *Covered telecommunications and video surveillance*. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) at *https://www.sam.gov* for entities excluded from receiving federal awards for “covered telecommunications equipment or services.”

(2) *FASCSA Orders*.

(i) The Offeror shall search in SAM for the phrase “FASCSA order” for any covered article, or any products or services produced or provided by a source, if there is an applicable FASCSA order described in paragraph (e) of FAR 52.240-91, Security Prohibitions and Exclusions.

(ii) The Offeror shall review the solicitation for any FASCSA orders that are not in SAM but are effective and apply to the solicitation and resultant contract (see FAR 40.204-1(c)(2)).

(iii) FASCSA orders issued after the date of solicitation do not apply unless added by an amendment to the solicitation.

(c) *Covered telecommunications equipment or services representations*. By submission of its offer, the Offeror represents that, after conducting a reasonable inquiry (that looks at any information in the Offeror’s possession but does not need to include an internal or third-party audit)—

(1) It will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation, except as waived by the solicitation, or as disclosed in paragraph (g); and

(2) It does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services, except as waived by the solicitation, or as disclosed in paragraph (g).

(d) *FASCSA Representation*. By submission of this offer, the offeror represents that it has conducted a reasonable inquiry, and that the offeror does not propose to provide or use in

response to this solicitation any covered article, or any products or services produced or provided by a source, if the covered article or the source is prohibited by an applicable FASCSA order in effect on the date the solicitation was issued, except as waived by the solicitation, or as disclosed in paragraph (g). A reasonable inquiry will look at any information in the offeror's possession but does not need to include an internal or third-party audit.

(e) *Sudan certification*. By submission of its offer, the offeror certifies, after conducting a reasonable inquiry (that looks at any information in the offeror's possession but does not need to include an internal or third-party audit), that the offeror does not conduct any restricted business operations in Sudan.

(f) *Iran Representation and Certifications*.

(1) Except as provided in paragraph (f)(2) of this provision or if a waiver has been granted in accordance with FAR 40.203-3, the offeror, after conducting a reasonable inquiry (that looks at any information in the offeror's possession but does not need to include an internal or third-party audit), by submission of its offer—

(i) Represents, to the best of its knowledge and belief, that the offeror does not export any sensitive technology to the government of Iran or any entities or individuals owned or controlled by, or acting on behalf or at the direction of, the government of Iran;

(ii) Certifies that the offeror, or any person (as defined at section 15 of the Iran Sanctions Act of 1996, Pub. L. 104-172, 50 U.S.C. 1701 note) owned or controlled by the offeror, does not engage in any activities for which sanctions may be imposed under section 5 of the Act. These sanctioned activities are in the areas of development of the petroleum resources of Iran, production of refined petroleum products in Iran, sale and provision of refined petroleum products to Iran, and contributing to Iran's ability to acquire or develop certain weapons or technologies; and

(iii) Certifies that the offeror, and any person owned or controlled by the offeror, does not knowingly engage in any transaction that exceeds $15,000 with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (see OFAC's Specially Designated Nationals and Blocked Persons List at *https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx*)

(2) Exception for trade agreements. The representation and certification requirements of paragraph (f)(1) of this provision do not apply if—

(i) This solicitation includes a trade agreements notice or certification (e.g., 52.225-6, Trade Agreements Certificate); and

(ii) The offeror has certified that all the offered products to be supplied are designated country end products or designated country construction material.

(iii) The offeror shall email questions concerning sensitive technology to the Department of State at *CISADA106@state.gov*.

(g) *Disclosure*.

(1) If the Offeror is not able to represent compliance with the prohibitions in paragraphs (c) or (d), then the Offeror shall disclose within 72 hours to the contracting office identified in paragraph (g)(2) the following information for each product or service not compliant:

(i) Contract number and order number, if applicable;

(ii) Identification of whether this disclosure relates to paragraph (c) on covered telecommunication equipment or services, or to paragraph (d) on FASCSA orders;

(iii) A description of the products or services that the Contractor identifies or has reason to suspect is prohibited (include brand; model number, such as the original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);

(iv) The entity that produced the product or service (include entity name, unique entity identifier, Contractor and Government Entity (CAGE) code, facilities responsible for design, fabrication, assembly, packaging, and test of the product, and whether the entity was the OEM or a distributor (provide manufacturer codes and distributor codes used for the product));

(v) Description of the functionality of the product or service and how that functionality impacts the risk to the product or service;

(vi) An explanation of any factors relevant to determining if the product or service should be permitted by an applicable exception, exemption, or waiver (if the offeror would like the Government to consider a waiver);

(vii) Whether alternative products or services are available that would be compliant with the prohibition;

(viii) If the product or service is related to item maintenance, include the following information on the item being maintained:

(A) Brand;

(B) Model number, OEM number, manufacturer part number, or wholesaler number; and

(C) Item description, as applicable.

(ix) Any readily available information about mitigation actions undertaken or recommended.

(2) If a disclosure is required to be submitted to a contracting office, the offeror shall submit the disclosure as follows:

(i) If a Department of Defense contracting office, the offeror shall submit the disclosure to the website at *https://dibnet.dod.mil*.

(ii) For all other contracting offices, the Offeror shall submit the disclosure to the Contracting Officer.

(3) If the disclosure provided does not contain any of the information required by paragraph (1), and the Offeror later discovers new information that is required by paragraph (1), then the Offeror shall submit a subsequent disclosure within 72 hours of discovering the new information.

(h) *Executive agency review of disclosures*. The Contracting Officer will review disclosures provided in paragraph (g) to determine if any applicable waiver may be sought. The Contracting Officer may choose not to pursue a waiver and may instead make an award to an Offeror that does not require a waiver.

(End of Provision)

E.9 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)

This solicitation incorporates one or more solicitation provisions 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. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es):

https://www.acquisition.gov/browse/index/far
https://www.va.gov/oal/library/vaar/

(End of Provision)

FAR Number	Title	Date
52.203-18	PROHIBITION ON CONTRACTING WITH ENTITIES THAT REQUIRE CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS—REPRESENTATION	JAN 2017
52.204-7	SYSTEM FOR AWARD MANAGEMENT—REGISTRATION (DEVIATION)	NOV 2025
52.214-21	DESCRIPTIVE LITERATURE	APR 2002
52.229-11	TAX ON CERTAIN FOREIGN PROCUREMENTS—NOTICE AND REPRESENTATION	JUN 2020
852.239-75	INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY NOTICE	FEB 2023

(End of Addendum to 52.212-1)