

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES				1. REQUISITION NO.		PAGE 1 OF	
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30							
2. CONTRACT NO.		3. AWARD/EFFECTIVE DATE		4. ORDER NO.		5. SOLICITATION NUMBER	
						36C24426Q0533	
						06-18-2026	
7. FOR SOLICITATION INFORMATION CALL:		a. NAME April Cotter				b. TELEPHONE NO. (No Collect Calls) 210-269-1927	
						8. OFFER DUE DATE/LOCAL TIME 06-29-2026 15:00 EDT	
9. ISSUED BY Department of Veterans Affairs Network Contracting Office 4 Services 2 1010 Delafield Rd. Pittsburgh PA 15215				CODE 00244			
				10. THIS ACQUISITION IS <input type="checkbox"/> UNRESTRICTED OR <input checked="" type="checkbox"/> SET ASIDE: 100 % FOR: <input type="checkbox"/> SMALL BUSINESS <input type="checkbox"/> WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM NAICS: 561621 <input type="checkbox"/> HUBZONE SMALL BUSINESS <input type="checkbox"/> EDWOSB <input checked="" type="checkbox"/> SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS <input type="checkbox"/> 8(A) Y \$25 Million			
11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED <input type="checkbox"/> SEE SCHEDULE		12. DISCOUNT TERMS		<input type="checkbox"/> 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)		13b. RATING N/A	
						14. METHOD OF SOLICITATION <input checked="" type="checkbox"/> RFQ <input type="checkbox"/> IFB <input type="checkbox"/> RFP	
15. DELIVER TO Department of Veterans Affairs Network Contracting Office 4 VA Pittsburgh Healthcare System (VAPHS) Pittsburgh PA 15240				CODE			
				16. ADMINISTERED BY Department of Veterans Affairs Network Contracting Office 4 Services 2 1010 Delafield Rd. Pittsburgh PA 15215			
17a. CONTRACTOR/OFFEROR		CODE		FACILITY CODE		18a. PAYMENT WILL BE MADE BY	
						CODE 00244	
						Austin Payment Center Department of Veterans Affairs PO Box 149971 Austin TX 78714-9971 PHONE: (877) 353-9791 FAX: (512) 460-5429	
TELEPHONE NO.		UEI:		EFT:			
<input type="checkbox"/> 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER				<input type="checkbox"/> 18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED <input type="checkbox"/> SEE ADDENDUM			
19. ITEM NO.		20. SCHEDULE OF SUPPLIES/SERVICES		21. QUANTITY		22. UNIT	
		See CONTINUATION Page				23. UNIT PRICE	
						24. AMOUNT	
		<p>The VA Pittsburgh Healthcare System (VAPHS) has a requirement for Security Systems Maintenance Services. All labor, equipment and travel to provide Security, Surveillance and Communications Systems Maintenance Services. The Contractor shall provide field service necessary to troubleshoot and maintain designated security, surveillance, and electronic systems at two campus locations in the Pittsburgh PA area.</p> <p>This solicitation will result in one FFP contract award.</p> <p>This is 100% SDVOSB Set-aside. Wage Determination 2015-4235 Rev 33, 03-30-2026 applies.</p> <p>All questions and quotes shall be submitted via email only to April.Cotter@va.gov Questions are due by 15:00 PM EST 06/25/2026 and Quotes are due by 15:00 PM EST 06/29/2026.</p> <p>(Use Reverse and/or Attach Additional Sheets as Necessary)</p>					
25. ACCOUNTING AND APPROPRIATION DATA See CONTINUATION Page						26. TOTAL AWARD AMOUNT (For Govt. Use Only)	
<input type="checkbox"/> 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA						<input checked="" type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED.	
<input type="checkbox"/> 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA						<input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED	
<input checked="" type="checkbox"/> 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN <u>1</u> 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				<input type="checkbox"/> 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) Stephanie Luniewski		31c. DATE SIGNED	

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 PRICE/COST SCHEDULE	5
ITEM INFORMATION.....	5
B.3 STATEMENT OF WORK.....	6
SECTION C - CONTRACT CLAUSES	23
C.1 IT CONTRACT SECURITY	23
C.2 52.212-4 Terms and Conditions—Commercial Products and Commercial Services. (Oct 2025).....	32
C.3 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999).....	38
C.4 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)... 38	
C.4 52.222-90 ADDRESSING DEI DISCRIMINATION BY FEDERAL CONTRACTORS APR 2026.....	38
C.5 52.240-91 SECURITY PROHIBITIONS AND EXCLUSIONS (NOV 2025) (DEVIATION).....	39
C.6 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)	48
C.7 SUPPLEMENTAL INSURANCE REQUIREMENTS	50
C.8 52.245-2 GOVERNMENT PROPERTY INSTALLATION OPERATION SERVICES (APR 2012).....	51
C.9 52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (NOV 2020)	51
C.10 VAAR 852.204-72 PERSONNEL VETTING AND CREDENTIALING (DEVIATION) (MAR 2026)	51
C.11 VAAR 852.222-71 COMPLIANCE WITH EXECUTIVE ORDER 13899 (DEVIATION)(APR 2025).....	55
SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS	56
SECTION E - SOLICITATION PROVISIONS	57
E.1 52.209-7 INFORMATION REGARDING RESPONSIBILITY MATTERS (OCT 2018)	57
E.2 52.212-1 INSTRUCTIONS TO OFFERORS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES. (OCT 2025).....	58
52.212-2 EVALUATION—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES. (OCT 2025)	59
E.3 52.212-3 OFFEROR REPRESENTATIONS AND CERTIFICATIONS— COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (OCT 2025) (DEVIATION FEB 2025)	61
E.4 52.219-1 SMALL BUSINESS PROGRAM REPRESENTATIONS (NOV 2025) (DEVIATION).....	78
E.5 52.233-2 SERVICE OF PROTEST (SEP 2006).....	80

E.6 52.240-90 SECURITY PROHIBITIONS AND EXCLUSIONS REPRESENTATIONS AND CERTIFICATIONS (NOV 2025) (DEVIATION).....	81
E.7 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998).....	85
E.8 52.252-5 AUTHORIZED DEVIATIONS IN PROVISIONS (NOV 2020).....	86

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 36C244

Department of Veterans Affairs

Network Contracting Office 4

Services 2

1010 Delafield Rd.

Pittsburgh PA 15215

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 ☒ In arrears, monthly after the completion of services.

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.

All invoices shall be submitted to Tungsten at <https://authentication.tungsten-network.com/login>

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

AMENDMENT NO	DATE

B.2 PRICE/COST SCHEDULE

ITEM INFORMATION

ITEM NUMBER	DESCRIPTION OF SUPPLIES/SERVIC ES	QUANTIT Y	UNI T	UNIT PRICE	AMOUNT
0001		12.00	MO		
	Security, Surveillance and Communication Systems Maintenance Services. Contract Period: Base POP Begin: POP End: PRINCIPAL NAICS CODE: 561621 - Security Systems Services (except Locksmiths) PRODUCT/SERVICE CODE: DJ01 - IT and Telecom - Security And Compliance Support Services (Labor)				
1001		12.00	MO		
	Security, Surveillance and Communication Systems Maintenance Services. Contract Period: Option 1 POP Begin: POP End: PRINCIPAL NAICS CODE: 561621 - Security Systems Services (except Locksmiths) PRODUCT/SERVICE CODE: DJ01 - IT and Telecom - Security And Compliance Support Services (Labor)				
2001		12.00	MO		
	Security, Surveillance and Communication Systems Maintenance Services. Contract Period: Option 2 POP Begin: POP End: PRINCIPAL NAICS CODE: 561621 - Security Systems Services (except Locksmiths) PRODUCT/SERVICE CODE: DJ01 - IT and Telecom -				

Security And Compliance Support Services (Labor)				
3001	12.00	MO	_____	_____
			—	—
Security, Surveillance and Communication Systems Maintenance Services. Contract Period: Option 3 POP Begin: POP End: PRINCIPAL NAICS CODE: 561621 - Security Systems Services (except Locksmiths) PRODUCT/SERVICE CODE: DJ01 - IT and Telecom - Security And Compliance Support Services (Labor)				
4001	12.00	MO	_____	_____
			—	—
Security, Surveillance and Communication Systems Maintenance Services. Contract Period: Option 4 POP Begin: POP End: PRINCIPAL NAICS CODE: 561621 - Security Systems Services (except Locksmiths) PRODUCT/SERVICE CODE: DJ01 - IT and Telecom - Security And Compliance Support Services (Labor)				
			GRAND TOTAL	_____
				—

B.3 STATEMENT OF WORK

VA Pittsburgh Healthcare System

Security, Surveillance and Communications Systems Services

Purpose

The VA Pittsburgh Healthcare System (VAPHS) has a requirement for all labor, equipment and travel to provide Security, Surveillance and Communications Systems Maintenance Services. The Contractor shall provide troubleshooting services and maintain designated security, surveillance, and electronic systems at two campus locations in the Pittsburgh PA area. Limited time may also be allocated to projects involved with installing new and upgraded systems. In some cases, most of the work involved with new and upgraded systems shall be performed by VAPHS staff and the Contractor shall provide service hours for material sourcing, final connections, troubleshooting and programming to complete projects.

Scope of Work

The Contractor shall provide services to include regular scheduled maintenance and emergency service calls when required.

1.1. Systems Description

Avigilon Network Based CCTV System:

- 1) Quarterly Maintenance performed on all serviceable Pelco/Endura appliances on the VAPHS network. This process includes firmware/software updates, server to system data management, and CCTV camera cleaning, adjusting and focusing.
- 2) Troubleshooting Services.
- 3) General maintenance on recording management for the NSM5200.
- 4) Assisting VAPHS to build risers to reflect point to point data for all Avigilon devices over the CCTV VLANs.

RS2 Access Control System:

- 1) Troubleshooting Services for all installed points.
- 2) Support for critical integration with Intrusion Detection and Hardwired Panic Buttons will be supported.
- 3) All existing Mercury hardware is Generation 2 and is now no longer being sold by RS2. Generation 3 hardware sets (EP & MR hardware). Contractor will advise and facilitate these repairs/upgrades as needed.

Emergency Call Stations:

Currently, Stentofon is utilized in the UD Parking Garage and AiPhone IS Series is utilized around the UD

Building 30 perimeter and under the Building 1 Bed Tower.

- 1) Although Stentofon's analog system is End of Life, there are still limited parts that can be procured to keep the system running until an upgrade to the whole system is completed.
- 2) AiPhone systems are still supported by the vendor and are IP based.
- 3) Code Blue is the Emergency Call system in place for the HZ Campus.
- 4) Contractor shall service all installed technology, within limits and support established by the manufacturers, to maximize the life span of these systems.

AiPhone Intercom Systems:

- 1) Contractor shall service all AiPhone technology to maximize the life span of this system. This also includes intercom stations that integrate with Access Control.

Bogen Overhead Paging System:

Although the Contractor may not be a Bogen-certified service provider, VAPHS is seeking a Contractor that can utilize general electronics maintenance knowledge and experience to maintain the overhead paging system including tasks as follows:

- 1) System troubleshooting and repair
- 2) Source parts through existing distributor channels
- 3) Perform preventive maintenance per manufacturers recommendations
- 4) Installation and replacement of system components including speakers, amplifiers, etc.

1.2. Preventive Maintenance Tasks for Specific Equipment Included in Contract

The following are mandatory tasks and associated deliverables to ensure that the systems are maintained in optimal working condition:

Workstations:

1. Check for any mechanical loose connections.
2. Check for any electrical loose connections.
3. Check for connections to RS232 or TC/PIP.
4. Check for Modem Operation.
5. Test for proper voltages on power supply.
6. Run Diagnostics on Security Application.
7. Run Indexing on database if applicable.
8. Check for proper AC voltage input, it must be connected to a dedicated circuit only.
9. Check for proper version level on the security application and update any files needed if available for the operating system.
10. Back Up entire Security System and check previous back up files.

Intrusion Detection System:

1. Check for Alarm Message Paging Software with live alarm tests.
2. Check for Modem Operation.

3. Check for connections to RS232 or TC/PIP.
4. Test all Alarm Sensors.
5. Test all Door Contacts.
6. Test all Motion Detectors.
7. If the IDS system uses a PC, you need to check for proper version level on the security application and update any files needed if available for the operating system.
8. Back Up entire Security files and check previous back up files.

HUB, Switch and Router:

1. Check Fan for proper movement and clean filters.
2. Check for any mechanical loose connections.
3. Run Diagnostics from the Communication's Application if applicable.

Microcontroller, Channel Expander and Multiplexers:

1. Check Fan for proper movement, clean filters.
2. Check for any mechanical loose connections.
3. Check for any electrical loose connections.
4. Check for connections to RS232, Current Loop, RS485, Wiegand or TC/PIP.
5. Check all plug-in connectors for loose data wires.
6. Test proper voltages on power supply, clean voltage no ripple on scope +/-5vdc and +/- 12 vdc.
7. Run Diagnostics from the Security Application if applicable.
8. Download, Reload or Reallocate the Database to the Controller.

Power Supplies and Battery Backups:

1. Check for proper AC voltage input, it must be connected to a dedicated circuit only.
2. Check for proper DC voltage input, from Battery Backup Circuitry.
3. Assist to develop/maintain Replacement Schedule Power Supply and battery replacements, every two (2) years. Review battery replacement procedure with VA electronics technicians.

4. Test for proper voltages on power supply, look for clean voltage look for no ripple on scope

+5vdc and +12 vdc.

Reader and Reader Interface:

1. Check for any mechanical loose connections.
2. Check for any electrical loose connections.
3. Check for Data communication connectors.
4. Do a visual check for Relay contact, especially if it is connected to a Gate Operator.
5. Check for any loose connections to ground.
6. Test voltages on power supply circuitry, clean voltage look ripple on scope +5vdc and +12 vdc.
7. Test for Input and Output signals, and intermediate relays.

Life Safety System:

1. Check for Fire Alarm Interface Connection, do a Test with Fire Alarm System, coordinate this test with building engineer.
2. Check for any mechanical loose connections.
3. Check for any electrical loose connections.
4. Check for control cable communication connectors.
5. Check for any debris or oil residues in the Mortise Lockset, make the necessary adjustments.
6. Adjust and make necessary adjustments to solenoid in the Mortise Lockset.
7. Adjust Magnetic Lock strike plate.
8. Test for Battery Backup for proper voltage levels.
9. Replace batteries every two years.
10. Test for proper output from reader or reader interface.
11. Test for proper operation on Master Intercom.
12. Test for proper operation on Intercom station.

Door Strikes, Door Contact, and Electromechanical Door Hardware:

1. Check for any mechanical loose connections.
2. Check for any electrical loose connections.
3. Check for control cable communication connectors.
4. Check for any debris or oil residues in the mechanical moving parts of the door strike, make the necessary adjustments.
5. If necessary, adjust and make necessary adjustments to solenoid in the door strike.
6. Adjust the strike plate.
7. Have the door closers adjusted for proper operation by building manager.
8. Look for any physical damage on the door hardware and make the necessary adjustments.

1.3. Documentation

Contractor shall establish, maintain, and update documentation for all work performed. When existing documentation is inadequate, the Contractor shall assist VAPHS with reviews of existing documentation and revise documentation methods and format as mutually agreed upon by the Contractor and the POC. Documentation shall include hard copies and electronic access to systems components including, but not limited to:

- equipment name, make and model
- manufacturer
- serial number
- physical location where installed
- door and area supported
- alarm modes
- associated (linked) equipment and settings
- wiring/schematic diagrams

The Contractor shall track all work hours in a service report to be submitted each week to the POC. The report shall state the number of hours worked and the specific equipment and systems that were serviced. The report shall also include the equipment condition as found, actions taken, and either confirmation of completion or additional actions that are required.

1.4. Scheduled Work Hours

The Contractor shall provide most service hours between 7:00 a.m. and 4:00 p.m. Monday through Friday. The Contractor may be required to provide services outside of normal business hours.

1.5. Emergency Work Hours

Contractor shall provide 24/7/365 emergency contact information for emergent work required outside of normally scheduled hours. The Contractor shall dispatch a technician in response to an emergency request by 7:00 a.m. on the first regular business day following the request.

1.6. Special Purpose System Vulnerability

For all systems covered by this Contract, the Contractor shall respond immediately in the event of a suspected information security breach, computer virus or malicious code that could spread to other systems and devices connected to the VA computer network. The Contractor shall immediately assist VAPHS to remove the affected system from the network as necessary, determine the cause of the incident and establish a plan to address and remediate the issue. The Contractor shall also take longer-term actions to address potential vulnerabilities.

Safety Requirements

1. The Contractor shall adhere to all OSHA, EPA, NFPA Life Safety Codes, and all other regulatory requirements.
2. In performance of this contract, the Contractor shall follow VAPHS safety policies and standards for safe work practices and take such safety precautions as the VAPHS Safety Officer or designee may determine to be reasonably necessary to protect the lives and health of occupants of VAPHS facilities. The Contractor shall comply with VAPHS smoking policy, which designates that all VAPHS property as non-smoking and non-vaping areas.
3. The Contractor shall submit to the POC, prior to the start of the contract, the Material Safety Data Sheets (MSDS) for all potentially hazardous materials (lubricants, cleaners, working fluids, etc.) to be used in VAPHS facilities during performance of the contract, and shall not use in VAPHS facilities, any materials which have not been cleared for use in advance with the POC. MSDS for new chemicals shall be furnished concurrently with the arrival of the chemical on site. The Contractor shall maintain a copy of all MSDS at the chemical storage site in a location accessible to VAPHS personnel to assure compliance with all laws and requirements regarding the "Right to Know" law.
4. The Contractor is responsible for identifying, providing and maintaining all personal protective equipment (PPE) required to perform the duties outlined in the contract. Additionally, the Contractor is responsible for identifying and adhering to all applicable safety program guidelines (lockout/tag out, confined space entry, universal precautions, etc.) required to perform the work. Contractor is responsible for providing and documenting all required safety training and proper use of PPE to their employees.

5. The Contractor shall obtain a Hot Work Permit from the VAPHS Safety Office whenever soldering, welding, using a cutting torch, or other open flame, spark, or heat producing equipment is required. The Contractor is required to follow all requirements outlined for the issuance of the Hot Work Permit.
6. The Contractor shall provide the following information within ten (10) working days after award of the contract:
 - a. A detailed listing of safety programs and procedures that will be followed by the Contractor during the performance of the contract, and the work activities indicating when such procedures would be required.
 - b. The Contractor is responsible for the supervision of all its employees while on government property.
7. Asbestos. Fire Alarm System maintenance and repair may impact asbestos containing materials (ACM). ACM is often found in sprayed-on fireproofing (on ceiling slabs, and support beams); insulation (on pipes, valves, boilers) and within wall materials. The Government shall inform the Contractor of a known ACM in an individual building. If the Contractor must disturb materials he suspects may contain ACM, the Contractor shall immediately report it to the Technical Point of Contact (TPOC), and the TPOC shall investigate and instruct the Contractor how to avoid an airborne asbestos exposure.
8. Lead-Based Paint. Fire Alarm System maintenance and repair may impact lead-based paint. The Government shall inform the Contractor of any known lead-based paint in an individual building. If the Contractor must disturb materials he suspects may contain lead-based paint, the Contractor shall immediately report it to the TPOC and the TPOC shall investigate and instruct the Contractor how to avoid lead-based paint contamination.

Work Locations

Contractor shall perform work at locations as follows:

1. H.J. Heinz Progressive Care Center
1010 Delafield Rd
Pittsburgh, PA 15215
2. University Drive Division Medical Center
University Drive C
Pittsburgh, PA 15240
3. VA Pittsburgh Human Engineering Research Laboratory (HERL)
6425 Penn Ave., Suite 400 (Bakery Square)
Pittsburgh, PA 15206

4. PWC Property Solutions, LLC
3 Parkway Center, Building 3 ground floor
875 Green tree Road,
Pittsburgh, PA 15220
5. Monroeville VA Clinic
421 Mall Circle Drive
Monroeville, PA 15146

Contractor Personnel Security Requirements

1. VA shall coordinate with Veterans Service Center (VSC) to process necessary contractor security clearances and Personal Identity Verification (PIV) badges. Contractor shall cooperate fully with these processes.
2. Contractors shall be required to obtain a VA Personal Identification Verification (PIV) credential in accordance with VAPHS Policy. PIV badges are required for all Contract employees on-site. The PIV card serves as a VA ID badge and must always be worn.
3. Public Trust Background Investigation (BI) Security Clearance is required for contractor employees requiring access to data closets, data centers and VA network-connected computer workstations. At least one Contract employee on-site shall have a BI clearance.
4. A BI clearance is required to be granted elevated privileges. Contractor must be approved for elevated privileges for tasks requiring administrative rights on VA network workstations and servers. The Contractor shall comply with all OI&T requirements and staff directives involving use of VA computer equipment.
5. The Contractor shall meet all VA requirements to obtain/maintain computer access. Contractor staff must login to the VA network, including servers and using individual user accounts. Contractors shall not login and perform work using a service account.
6. Contractor-owned computer equipment including laptops are not permitted to be connected to the VA network. An MOU-ISA is required for any remote connection required between a contractor-owned system and the VA network.
7. Contractor employee(s) must sign Appendix D Contractor Rules of Behavior and must complete "VA Privacy and Information Security Awareness and Rules of Behavior" and "Privacy and HIPAA Focused Training" courses prior to the performance of the contract and annually thereafter. Training must be completed in VA's TMS system <https://www.tms.va.gov/>. Contractors must use the TMS Managed Self Enrollment method to complete the training in TMS. The TPOC shall ensure that all contractors are validated in the PIH domain. Proof of training completion shall be verified and tracked by the TPOC.

8. The Contractor shall not have access to any VA sensitive information under this contract.

VA Healthcare Directives

1. The Contractor shall comply with the requirements of the following VA Healthcare Directives:
 - a. Tuberculosis Screening- VHA Directive 2011-036, *Safety and Health During Construction*. Contractor must certify annually to the TPOC(s) that all Contractor employees working at VAPHS facilities have a documented screening for latent Tuberculosis within the last 12 months. If screening for latent Tuberculosis is positive, clearance from a physician is required prior to working at VAPHS. Contractor employees that fail to meet this requirement will not be permitted to work at VAPHS facilities and may be asked to leave VAPHS property without notice until the requirement is met.
 - b. Seasonal Influenza Vaccination - VHA Directive 1192, *Seasonal Influenza Prevention Program for VHA Health Care Personnel*. Contractor shall certify annually to the TPOC(s) that all employees working at VAPHS facilities have received a seasonal influenza vaccination.

HEALTH CARE PERSONNEL INFLUENZA VACCINATION FORM

☐ I received the seasonal influenza vaccine this flu season (required documentation is attached.)

☐ I decline to receive seasonal influenza vaccine at this time for the following reason:

Select the single answer that best fits your reason:

☐ I do not like needles.

☐ I have a philosophical or religious reason for not receiving the vaccine.

☐ I have an allergy to the vaccine or one of its components.

☐ I am concerned about the side effects/safety of the vaccine.

☐ I have never had the flu and don't think I will this season.

☐ I have another reason. (Please explain)

I acknowledge that VHA policy requires health care personnel to receive the influenza vaccine every year. I understand that if I decline to receive the vaccine and/or to provide proof of vaccination by November 30 or within two weeks of beginning employment if after November 30, I must wear a face mask according to requirements and guidelines within the Directive 1192, Seasonal Influenza Prevention Program.

I have read and fully understand the information on this form and have been given the opportunity to have my questions answered.

Signature: _____ Date: _____

Name (print): _____ Last 4 SS# _____

Contractor Name: _____

Access to VA Information and VA Information Systems:

- a. A contractor/subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.
- b. All contractors, subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors must be in accordance with VA Directive and Handbook 0710, Personnel Suitability and Security Program. The Office of Operations, Security, and Preparedness is responsible for these policies and procedures.
- c. The contractor or subcontractor must notify the Contracting Officer (CO) immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the contractor or subcontractor's employ. The Contracting Officer must also be notified immediately by the contractor or subcontractor prior to an unfriendly termination.

VA Information Custodial Language

- a. Information made available to the Contractor or subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the Contractor/subcontractor's rights to use data as described in Rights in Data – General, FAR 52.227-14(d) (1).
- b. VA information should not be co-mingled, if possible, with any other data on the contractors/subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the contractor must ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on-site inspections of contractor and subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedure are in compliance with VA directive requirements.
- c. Prior to termination or completion of this contract, contractor/subcontractor must not destroy information received from VA, or gathered/created by the contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of VA by a contractor/subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization. Self-certification by the contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.

d. The contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable

Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality

and security laws, regulations and policies in this contract.

e. The contractor/subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on contractor/subcontractor electronic storage media for restoration in case any electronic equipment or data used by the contractor/subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

f. If VA determines that the contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

g. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor/subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The contractor/subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

h. Notwithstanding the provision above, the contractor/subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the contractor/subcontractor is in receipt of a court order or other request for the above mentioned information, that contractor/subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

i. For services that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or an MOU-ISA for system interconnection, the contractor/subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COTR

Information System Design and Development

a. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R.

Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA

Handbook 6500, VA Information Security Program). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COTR, and approved by the VA Privacy Service in accordance with Directive 6507, VA Privacy Impact Assessment.

b. The contractor/subcontractor shall certify to the COTR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or the VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.

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

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

e. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, VA Handbook 6500, Information Security

Program and VA Handbook 6500.5, Incorporating Security and Privacy in System Development Lifecycle.

f. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as "Systems"), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hotfixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published

or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

g. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, but in no event longer than 3 days.

h. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to the VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes within 3 days.

i. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the contracting officer and the VA Assistant Secretary for Office of Information and Technology.

Information System Hosting, Operation, Maintenance, or Use

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, contractors/subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion

of an acceptable contingency plan for each system. The contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COTR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA's network involving VA information must be reviewed and approved by VA prior to implementation.

b. The contractor/subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer and the ISO for entry into VA's POA&M management process. The contractor/subcontractor must use VA's POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities.

Security deficiencies must be corrected within the timeframes approved by the government. Contractor/subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with contractor/subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the

C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

c. The contractor/subcontractor must conduct an annual self-assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COTR. The government reserves the right to conduct such an assessment using government personnel or another contractor/subcontractor. The contractor/subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

d. VA prohibits the installation and use of personally-owned or contractor/subcontractor-owned equipment or software on VA's network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of

the security controls required for government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non- VA owned OE.

e. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, Electronic Media Sanitization upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the contractor/subcontractor or any person acting on behalf of the contractor/subcontractor, whichever is earlier. Media (hard drives, optical disks,

CDs, back-up tapes, etc.) used by the contractors/subcontractors that contain VA information must be returned to the VA for sanitization or destruction or the contractor/subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

Security Incident Investigation

a. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/subcontractor shall immediately notify the COTR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained system(s) to which the Contractor/subcontractor has access.

b. To the extent known by the contractor/subcontractor, the contractor/subcontractor’s notice to VA

shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised),

and any other information that the contractor/subcontractor considers relevant.

Security Controls Compliance Testing

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the contractor under the clauses contained within the contract. With 10 working-days’ notice, at the request of the government, the contractor must fully cooperate and assist in a government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

Training

a. All Contractor employees and subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems.

(1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the Contractor Rules of Behavior, Appendix E relating to access to VA information and information systems;

(2) Successfully complete the VA Cyber Security Awareness and Rules of Behavior training and annually complete required security training.

(3) Successfully complete the appropriate VA privacy training and annually complete required privacy training; and

(4) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access [to be defined by the VA program official and provided to the contracting officer for inclusion in the solicitation document – e.g., any role based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]

b. The Contractor shall provide to the Contracting Officer and/or the COTR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

Appendix D

Before being granted access to VA information or information systems, all contractor employees and subcontractor employees requiring such access must sign the VA's Contractor Rules of Behavior. Contractor must complete "VA Privacy and Information Security Awareness and Rules of Behavior" training prior to the performance of the contract and annually thereafter. Training must be completed in VA's TMS system (<https://www.tms.va.gov/SecureAuth35/>).

Contractors must use the TMS Managed Self Enrollment method to complete the training in TMS. The TPOC must ensure that all contractors are validated in the PIH domain. Proof of training completion must be verified and tracked by the TPOC.

SECTION C - CONTRACT CLAUSES

C.1 IT CONTRACT SECURITY

VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY

1. GENERAL

Contractors, contractor personnel, subcontractors, and subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A contractor/subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

b. All contractors, subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors must be in accordance with VA Directive and Handbook 0710, Personnel Suitability and Security Program. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the contractor/subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e. The contractor or subcontractor must notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the contractor or subcontractor's employ. The Contracting Officer must also be notified immediately by the contractor or subcontractor prior to an unfriendly termination.

3. VA INFORMATION CUSTODIAL LANGUAGE

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

b. VA information should not be co-mingled, if possible, with any other data on the contractors/subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the contractor must ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of contractor and subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

c. Prior to termination or completion of this contract, contractor/ subcontractor must not destroy information received from VA, or gathered/ created by the contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of VA by a contractor/subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization. Self-certification by the contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.

d. The contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

e. The contractor/subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on contractor/subcontractor electronic storage media for restoration in case any electronic equipment or data used by the contractor/subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

f. If VA determines that the contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

g. If a VHA contract is terminated for cause, the associated BAA must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, Business Associate Agreements. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

h. The contractor/subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

i. The contractor/subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.

j. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor/subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The contractor/subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

k. Notwithstanding the provision above, the contractor/subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the contractor/subcontractor is in receipt of a court order or other requests for the above mentioned information, that contractor/subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

l. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or an MOU-ISA for system interconnection, the contractor/subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

a. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, VA Information Security Program). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6507, VA Privacy Impact Assessment.

b. The contractor/subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or the VA. This

includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.

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

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

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

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

g. The contractor/subcontractor agrees to:

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

(a) The Systems of Records (SOR); and

(b) The design, development, or operation work that the contractor/ subcontractor is to perform;

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

(2) Include this Privacy Act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR.

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

(1) "Operation of a System of Records" means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.

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

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

i. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as "Systems"), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hotfixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

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

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

l. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the contracting officer and the VA Assistant Secretary for Office of Information and Technology.

5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, contractors/subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA

Privacy Service prior to operational approval. All external Internet connections to VA's network involving VA information must be reviewed and approved by VA prior to implementation.

b. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

c. Outsourcing (contractor facility, contractor equipment or contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization) (C&A) of the contractor's systems in accordance with VA Handbook 6500.3, Certification and Accreditation and/or the VA OCS Certification Program Office. Government- owned (government facility or government equipment) contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

d. The contractor/subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer and the ISO for entry into VA's POA&M management process. The contractor/subcontractor must use VA's POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the government. Contractor/subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with contractor/ subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the C&A of the system may need to be reviewed, retested and re- authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

e. The contractor/subcontractor must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The government reserves the right to conduct such an assessment using government personnel or another contractor/subcontractor. The contractor/subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

f. VA prohibits the installation and use of personally-owned or contractor/ subcontractor-owned equipment or software on VA's network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the

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

g. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, Electronic Media Sanitization upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the contractor/subcontractor or any person acting on behalf of the contractor/subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the contractors/ subcontractors that contain VA information must be returned to the VA for sanitization or destruction or the contractor/subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

h. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

- (1) Vendor must accept the system without the drive;
- (2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or
- (3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

(4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for the VA to retain the hard drive, then;

(a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and

(b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be pre-approved and described in the purchase order or contract.

(c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

6. SECURITY INCIDENT INVESTIGATION

a. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that

breaches VA security procedures. The contractor/ subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/ subcontractor has access.

b. To the extent known by the contractor/subcontractor, the contractor/ subcontractor's notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the contractor/subcontractor considers relevant.

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. In instances of theft or break-in or other criminal activity, the contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The contractor, its employees, and its subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The contractor/subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

7. LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. 5725, a contract may require access to sensitive personal information. If so, the contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the contractor/subcontractor processes or maintains under this contract.

b. The contractor/subcontractor shall provide notice to VA of a "security incident" as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

c. Each risk analysis shall address all relevant information concerning the data breach, including the following:

- (1) Nature of the event (loss, theft, unauthorized access);

(2) Description of the event, including:

- (a) date of occurrence;
- (b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
- (3) Number of individuals affected or potentially affected;
- (4) Names of individuals or groups affected or potentially affected;
- (5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
- (6) Amount of time the data has been out of VA control;
- (7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
- (8) Known misuses of data containing sensitive personal information, if any;
- (9) Assessment of the potential harm to the affected individuals;
- (10) Data breach analysis as outlined in 6500.2 Handbook, Management of Security and Privacy Incidents, as appropriate; and
- (11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

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

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

8. SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the contractor under the clauses contained within the contract. With 10 working-day's notice, at the request of the government, the contractor must fully cooperate and assist in a government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

9. TRAINING

a. All contractor employees and subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

(1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the Contractor Rules of Behavior, Appendix E relating to access to VA information and information systems;

(2) Successfully complete the VA Cyber Security Awareness and Rules of Behavior training and annually complete required security training;

(3) Successfully complete the appropriate VA privacy training and annually complete required privacy training; and

(4) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access [to be defined by the VA program official and provided to the contracting officer for inclusion in the solicitation document - e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]

b. The contractor shall provide to the contracting officer and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

(End of Clause)

C.2 52.212-4 Terms and Conditions—Commercial Products and Commercial Services. (Oct 2025)

(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)

C.3 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within /prior to 30 days..

(End of Clause)

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

(a) The Government may extend the term of this contract by written notice to the Contractor within /prior to 30 days.; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed five (5) years.

(End of Clause)

C.5 52.222-90 ADDRESSING DEI DISCRIMINATION BY FEDERAL CONTRACTORS 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.6 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.7 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)

<u>FAR Number</u>	<u>Title</u>	<u>Date</u>
52.203-6	RESTRICTIONS ON SUBCONTRACTOR SALES TO THE GOVERNMENT	JUN 2020
52.203-13	CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT	NOV 2021
52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS	NOV 2023
52.203-19	PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS	JAN 2017
52.204-9	PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL	JAN 2011
52.204-13	SYSTEM FOR AWARD MANAGEMENT—MAINTENANCE (DEVIATION)	NOV 2025
52.209-6	PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, PROPOSED FOR DEBARMENT, OR VOLUNTARILY EXCLUDED	JAN 2025
52.209-9	UPDATES OF PUBLICLY AVAILABLE INFORMATION REGARDING RESPONSIBILITY MATTERS	OCT 2018
52.209-10	PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS	NOV 2015
52.219-6	NOTICE OF TOTAL SMALL BUSINESS SET-ASIDE (DEVIATION)	NOV 2025
52.219-8	UTILIZATION OF SMALL BUSINESS CONCERNS (DEVIATION)	NOV 2025
52.219-28	POSTAWARD SMALL BUSINESS PROGRAM REREPRESENTATION (DEVIATION)	NOV 2025
52.222-3	CONVICT LABOR (DEVIATION)	NOV 2025
52.222-35	EQUAL OPPORTUNITY FOR VETERANS (DEVIATION)	NOV 2025
52.222-36	EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES (DEVIATION)	NOV 2025
52.222-37	EMPLOYMENT REPORTS ON VETERANS (DEVIATION)	NOV 2025
52.222-40	NOTIFICATION OF EMPLOYEE RIGHTS UNDER THE NATIONAL LABOR RELATIONS ACT (DEVIATION)	NOV 2025
52.222-41	SERVICE CONTRACT LABOR STANDARDS (DEVIATION)	NOV 2025
52.222-43	FAIR LABOR STANDARDS ACT AND SERVICE CONTRACT LABOR STANDARDS-PRICE ADJUSTMENT (MULTIPLE YEAR AND OPTION CONTRACTS) (DEVIATION)	NOV 2025
52.222-44	FAIR LABOR STANDARDS ACT AND SERVICE CONTRACT LABOR STANDARDS—PRICE ADJUSTMENT (DEVIATION)	NOV 2025
52.222-50	COMBATING TRAFFICKING IN PERSONS (DEVIATION)	NOV 2025
52.222-54	EMPLOYMENT ELIGIBILITY VERIFICATION (DEVIATION)	NOV 2025
52.222-55	MINIMUM WAGES FOR CONTRACTOR WORKERS UNDER EXECUTIVE ORDER 14026 (DEVIATION)	NOV 2025

52.222-62	PAID SICK LEAVE UNDER EXECUTIVE ORDER 13706 (DEVIATION)	NOV 2025
52.223-5	POLLUTION PREVENTION AND RIGHT-TO-KNOW INFORMATION	MAY 2024
52.223-23	SUSTAINABLE PRODUCTS (DEVIATION)	NOV 2025
52.226-8	ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING	MAY 2024
52.228-5	INSURANCE—WORK ON A GOVERNMENT INSTALLATION	JAN 1997
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
52.237-2	PROTECTION OF GOVERNMENT BUILDINGS, EQUIPMENT, AND VEGETATION	APR 1984
52.244-6	SUBCONTRACTS FOR COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (DEVIATION)	APR 2026
52.245-1	GOVERNMENT PROPERTY ALTERNATE I (APR 2012)	SEP 2021
52.245-9	USE AND CHARGES	APR 2012
852.203-70	COMMERCIAL ADVERTISING	MAY 2018
852.204-70	PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL (DEVIATION)	MAR 2026
852.211-70	EQUIPMENT OPERATION AND MAINTENANCE MANUALS	NOV 2018
852.219-70	VA SMALL BUSINESS SUBCONTRACTING PLAN MINIMUM REQUIREMENTS	NOV 2022
852.232-72	ELECTRONIC SUBMISSION OF PAYMENT REQUESTS	NOV 2018
852.239-73	INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE	FEB 2023
852.239-74	SECURITY CONTROLS COMPLIANCE TESTING	FEB 2023

C.8 SUPPLEMENTAL INSURANCE REQUIREMENTS

In accordance with FAR 28.307-2 and FAR 52.228-5, the following minimum coverage shall apply to this contract:

(a) Workers' compensation and employers liability: Contractors are required to comply with applicable Federal and State workers' compensation and occupational disease statutes. If occupational diseases are not compensable under those statutes, they shall be covered under the employer's liability section of the insurance policy, except when contract operations are so commingled with a Contractor's commercial operations that it would not be practical to require this coverage. Employer's liability coverage of at least \$100,000 is required, except in States with exclusive or monopolistic funds that do not permit workers' compensation to be written by private carriers.

(b) General Liability: \$500,000.00 per occurrences.

(c) Automobile liability: \$200,000.00 per person; \$500,000.00 per occurrence and \$20,000.00 property damage.

(d) The successful bidder must present to the Contracting Officer, prior to award, evidence of general liability insurance without any exclusionary clauses for asbestos that would void the general liability coverage.

(End of Clause)

C.9 52.245-2 GOVERNMENT PROPERTY INSTALLATION OPERATION SERVICES (APR 2012)

(a) This Government Property listed in paragraph (e) of this clause is furnished to the Contractor in an "as-is, where is" condition. The Government makes no warranty regarding the suitability for use of the Government property specified in this contract. The Contractor shall be afforded the opportunity to inspect the Government property as specified in the solicitation.

(b) The Government bears no responsibility for repair or replacement of any lost Government property. If any or all of the Government property is lost or becomes no longer usable, the Contractor shall be responsible for replacement of the property at Contractor expense. The Contractor shall have title to all replacement property and shall continue to be responsible for contract performance.

(c) Unless the Contracting Officer determines otherwise, the Government abandons all rights and title to unserviceable and scrap property resulting from contract performance. Upon notification to the Contracting Officer, the Contractor shall remove such property from the Government premises and dispose of it at Contractor expense.

(d) Except as provided in this clause, Government property furnished under this contract shall be governed by the Government Property clause of this contract.

(e) Government property provided under this clause:

(End of Clause)

C.10 52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (NOV 2020)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

(b) The use in this solicitation or contract of any VAAR (48 CFR Chapter FEDERAL ACQUISITION REGULATION (48 CFR Chapter 1)) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of Clause)

C.11 VAAR 852.204-72 PERSONNEL VETTING AND CREDENTIALING (DEVIATION) (MAR 2026)

(a) Definitions. As used in this clause –

VA Information system is the same as information system and means, pursuant to 38 U.S.C. 5727, a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information whether automated or manual.

VA sensitive information means all VA data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information and includes sensitive personal information. The term includes information where improper use or disclosure could adversely affect the ability of VA to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of Federal programs.

(b) *General*. Contractor personnel assigned to work for or on behalf of VA must undergo a background investigation commensurate with the risk and sensitivity level designation associated with the work to be performed at the level indicated in the contract. The Contractor and subcontractors shall comply with VA Directive/Handbook 0710, Personnel Security and Suitability Program, which can be accessed at: <https://vaww.va.gov/vapubs/index.cfm>.

(c) *Risk and Sensitivity Levels*. The following table identifies the risk and sensitivity levels that apply to any personnel providing services under this contract. *VA Administrations, organizations and staff offices will use the OPM [Position Designation Tool](#).

Positions/Tasks Designated as Non-Sensitive Positions – Tier 1/Low Risk
Positions/Tasks Designated as Non-Sensitive Positions – Tier 2/Mod Risk

Positions/Tasks Designated as Non-Sensitive Positions – Tier 4/High Risk

Security clearances are granted to individuals with a specific requirement for access to classified material (for example, Confidential, Secret and Top Secret). Contractor personnel that are required to obtain a security clearance will be subject to a Tier 3 or Tier 5 investigation. The following sensitivity designations have been assigned for the identified Tier 3 and Tier 5 required by this contract:

Tier 3:

Tier 5:

(d) *Fitness*. The results from a background investigation are used to determine if an individual's fitness is sufficient for that individual to perform work for or on behalf of VA in the position identified in this contract. Contractor fitness determinations are made in accordance with 5 CFR Part 731.202.

Fitness requirements for employment are separate and distinct from job qualifications. If a Contractor or subcontractor employee is found to be unsuitable or unfit to provide services under this contract, the Contractor shall immediately remove the employee from working on this contract and take those necessary steps that restrict the employee's logical access to VA data, information, VA sensitive information, or information technology or VA information systems containing such data or information.

The Contractor shall advise the employee that they are not permitted to access any VA controlled building or real property in relation to this contract. The removal of an unfit Contractor or subcontractor employee does not alleviate the Contractor from satisfying the requirements of this contract. The Government will not reimburse the Contractor for any costs associated with the recruitment/replacement of an employee or subcontractor employee who is found to be unfit.

(e) *Identification Cards*. The Government will provide a Personal Identification Verification (PIV) card or other identification card, as necessary, to fit Contractor personnel who require physical access to VA facilities and/or logical access to VA data, information, VA sensitive information, or information technology or VA information systems containing such data or information. Contractor and subcontractor personnel shall prominently display their PIV/identification card on their persons while working at a VA facility and shall present their PIV/identification card for inspection upon request by a VA official. The Contractor must surrender the employee or subcontractor employee's PIV/identification card in accordance with the requirements set forth in Directive/Handbook 0735 when any of the following events occur:

1. When no longer needed for contract performance.
2. Upon completion of the Contractor/subcontractor employee's employment.
3. Upon contract completion or termination.

(f) *Lost/stolen*. Immediately upon detection, the Contractor shall report a lost or stolen PIV/identification card to the Government authorities as identified in Directive/Handbook 0735. Within 48 hours of reporting the lost/stolen PIV/identification card, the Contractor shall submit to the Program Manager an incident report that describes the relevant facts and circumstances regarding the loss/theft. If the loss/theft was reported by the Contractor to the local police, the Contractor shall further submit a copy of the final police report to the Program Manager within 48 hours of the report being made available by the local police department. The Government will not reimburse the Contractor for any costs that result from lost/stolen PIV/identification card(s).

(g) *Regular Reporting*. The Contractor shall submit a status report to PIV Sponsor within 5 working days after the end of each calendar quarter and as requested by the Government in order to initiate contract closeout procedures. The report must provide the status of each contractor/subcontractor employee who is required to have a PIV/identification card during the performance of the contract. The report shall identify the Contractor and the contract number, and list the following status for each contractor/subcontractor employee who holds a PIV/identification card under this contract:

1. Contractor/subcontractor employee name.
2. Name of VA facility where Contractor/subcontractor employee works, if applicable.
3. Date background check submitted for Contractor/subcontractor employee.
4. Date PIV/identification card issued to Contractor/subcontractor employee.
5. Contractor/subcontractor employee's PIV/identification card number, as applicable.
6. Date Contractor/subcontractor employee no longer has need for PIV/identification card.
7. Date Contractor notified VA that PIV/identification card is no longer required.
8. Date Contractor returned PIV/identification card was returned to VA.

(h) *Flow down of clause*. The Contractor shall include the substance of this clause in subcontracts, third-party agreements, and BAA's, in which subcontractors, third-party servicers/employees, and business associates will perform functions where they will have physical access to a VA facility or logical access to VA data, information, VA sensitive information, or information technology or VA information system containing such data or information.

(End of Clause)

C.12 VAAR 852.222-71 COMPLIANCE WITH EXECUTIVE ORDER 13899 (DEVIATION)(APR 2025)

(a) The contractor shall comply with Executive Order 13899, Combating Anti-Semitism, pursuant to Title VI of the Civil Rights Act of 1964 (Title VI), 42 U.S.C. 2000d et seq.

(b) The contractor shall timely disclose, in writing, to the Contracting Officer, whenever, in connection with the award, performance, or closeout of this contract or any subcontract thereunder, the Contractor has credible evidence that a principal, employee, agent, or subcontractor of the Contractor has committed a violation under Executive Order 13899, Combatting Anti-Semitism pursuant to the Civil Rights Act of 1964 (Title VI), 42 U.S.C. 2000d et seq.

(c) The contractor shall include the terms and conditions of this clause in every subcontract or purchase order so that these terms will be binding on every subcontractor or vendor.

(End of Clause)

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS

D.1 See attached document: 852.219-75 MUST SIGN AND RETURN WITH PROPOSAL.

D.2 See attached document: WD 2015-4235 Rev 33.

SECTION E - SOLICITATION PROVISIONS

E.1 52.209-7 INFORMATION REGARDING RESPONSIBILITY MATTERS (OCT 2018)

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

"Administrative proceeding" means a non-judicial process that is adjudicatory in nature in order to make a determination of fault or liability (e.g., Securities and Exchange Commission Administrative Proceedings, Civilian Board of Contract Appeals Proceedings, and Armed Services Board of Contract Appeals Proceedings). This includes administrative proceedings at the Federal and State level but only in connection with performance of a Federal contract or grant. It does not include agency actions such as contract audits, site visits, corrective plans, or inspection of deliverables.

"Federal contracts and grants with total value greater than \$10,000,000" means—

(1) The total value of all current, active contracts and grants, including all priced options; and

(2) The total value of all current, active orders including all priced options under indefinite-delivery, indefinite-quantity, 8(a), or requirements contracts (including task and delivery and multiple-award Schedules).

"Principal" means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (e.g., general manager; plant manager; head of a division or business segment; and similar positions).

(b) The offeror [] has [] does not have current active Federal contracts and grants with total value greater than \$10,000,000.

(c) If the offeror checked "has" in paragraph (b) of this provision, the offeror represents, by submission of this offer, that the information it has entered in the Federal Awardee Performance and Integrity Information System (FAPIIS) is current, accurate, and complete as of the date of submission of this offer with regard to the following information:

(1) Whether the offeror, and/or any of its principals, has or has not, within the last five years, in connection with the award to or performance by the offeror of a Federal contract or grant, been the subject of a proceeding, at the Federal or State level that resulted in any of the following dispositions:

(i) In a criminal proceeding, a conviction.

(ii) In a civil proceeding, a finding of fault and liability that results in the payment of a monetary fine, penalty, reimbursement, restitution, or damages of \$5,000 or more.

(iii) In an administrative proceeding, a finding of fault and liability that results in—

(A) The payment of a monetary fine or penalty of \$5,000 or more; or

(B) The payment of a reimbursement, restitution, or damages in excess of \$100,000.

(iv) In a criminal, civil, or administrative proceeding, a disposition of the matter by consent or compromise with an acknowledgment of fault by the Contractor if the proceeding could have led to any of the outcomes specified in paragraphs (c)(1)(i), (c)(1)(ii), or (c)(1)(iii) of this provision.

(2) If the offeror has been involved in the last five years in any of the occurrences listed in (c)(1) of this provision, whether the offeror has provided the requested information with regard to each occurrence.

(d) The offeror shall post the information in paragraphs (c)(1)(i) through (c)(1)(iv) of this provision in FAPIIS as required through maintaining an active registration in the System for Award Management, which can be accessed via <https://www.sam.gov> (see 52.204-7).

(End of Provision)

E.2 52.212-1 INSTRUCTIONS TO OFFERORS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES. (OCT 2025)

(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)

E.3 52.212-2 EVALUATION—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES. (OCT 2025)

Quote evaluation factors:

I. The Government will award a Firm-Fixed Price contract resulting from this solicitation to the responsible Offeror whose offer conforming to the solicitation will be most advantageous to the Government, price and other factors considered. The following factors shall be used to evaluate quotes:

(A) Price

(B) Technical Acceptability

(C) Compliance with quote submission instructions

(A) Price - Quoters are required to complete all line items in the solicitation. Line items shall not be edited. Pricing per unit and total per line are required as well as contract total.

(B) Technically Acceptability

(1) A quote will be deemed **Technically Acceptable** if it clearly meets all minimum requirements outlined in the Statement of Work (SOW).

(2) Public Trust Background Investigation (BI) Security Clearance is required for contractor employees requiring access to data closets, data centers and VA network-connected computer workstations. At least one Contract employee on-site shall have a BI clearance.

(C) Compliance with quote submission instructions

(1) **Questions are due** no later than 3:00 PM EST, Thursday June 25, 2026 to April Cotter at April.Cotter@va.gov.

(2) **Quotes shall be submitted** via email to April Cotter at April.Cotter@va.gov, Pamela Rayburg at Pamela.Rayburg@va.gov and Stephanie Luniewski at Stephanie.Luniewski@va.gov, no later than 3:00 PM EST, Monday June 29, 2026.

(3) In accordance with the Revolutionary FAR Overhaul (RFO) part 4.203-1(a), and RFO 52.204-7 (b)(1) quoters must be registered in the System for Award Management (SAM) database at time of quote submission **and** at time of award. Registration may be completed online at: www.acquisition.gov or www.sam.gov.

(4) Quoters must include the following in their submission:

- a. The solicitation number
- b. The deadline specified in the solicitation for receipt of offers
- c. The name, address, and telephone number of the quoter
- d. The SAM Unique Entity Identifier (UEI).

(5) In accordance with VAAR 819.7003(3) offerors must be registered in Veteran Small Business Certification (VetCert) run by the U.S. Small Business Administration database at time of quote submission and time of award. Registration may be done online at: <https://veterans.certify.sba.gov/>

(6) Quoters must complete VAAR 852.219-75 and return with submission. Note, only paragraph (a)(1)(i), Services, apply.

II. Evaluation of Quotations

(1) The Government intends to issue a firm-fixed price contract in response to this solicitation.

(2) An Evaluation of quotes will be performed in accordance with RFO 12.203.

E.4 52.212-3 OFFEROR REPRESENTATIONS AND CERTIFICATIONS— COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (OCT 2025) (DEVIATION FEB 2025)

The Offeror shall complete only paragraph (b) of this provision if the Offeror has completed the annual representations and certification electronically in the System for Award Management (SAM) accessed through <https://www.sam.gov>. If the Offeror has not completed the annual representations and certifications electronically, the Offeror shall complete only paragraphs (c) through (v) of this provision.

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

Covered telecommunications equipment or services has the meaning provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

Economically disadvantaged women-owned small business (EDWOSB) concern means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States and who are economically disadvantaged in accordance with 13 CFR 127, and the concern is identified by SBA or an approved third-party certifier in accordance with 13 CFR 127.300. It automatically qualifies as a women-owned small business eligible under the WOSB Program.

Forced or indentured child labor means all work or service—

(1) Exacted from any person under the age of 18 under the menace of any penalty for its nonperformance and for which the worker does not offer himself voluntarily; or

(2) Performed by any person under the age of 18 pursuant to a contract the enforcement of which can be accomplished by process or penalties.

Highest-level owner means the entity that owns or controls an immediate owner of the offeror, or that owns or controls one or more entities that control an immediate owner of the offeror. No entity owns or exercises control of the highest level owner.

Immediate owner means an entity, other than the offeror, that has direct control of the offeror. Indicators of control include, but are not limited to, one or more of the following: Ownership or interlocking management, identity of interests among family members, shared facilities and equipment, and the common use of employees.

Inverted domestic corporation means a foreign incorporated entity that meets the definition of an inverted domestic corporation under 6 U.S.C. 395(b), applied in accordance with the rules and definitions of 6 U.S.C. 395(c).

Manufactured end product means any end product in product and service codes (PSCs) 1000-9999, except—

- (1) PSC 5510, Lumber and Related Basic Wood Materials;
- (2) Product or Service Group (PSG) 87, Agricultural Supplies;
- (3) PSG 88, Live Animals;
- (4) PSG 89, Subsistence;
- (5) PSC 9410, Crude Grades of Plant Materials;
- (6) PSC 9430, Miscellaneous Crude Animal Products, Inedible;
- (7) PSC 9440, Miscellaneous Crude Agricultural and Forestry Products;
- (8) PSC 9610, Ores;
- (9) PSC 9620, Minerals, Natural and Synthetic; and
- (10) PSC 9630, Additive Metal Materials.

Place of manufacture means the place where an end product is assembled out of components, or otherwise made or processed from raw materials into the finished product that is to be provided to the Government. If a product is disassembled and reassembled, the place of reassembly is not the place of manufacture.

Predecessor means an entity that is replaced by a successor and includes any predecessors of the predecessor.

Reasonable inquiry has the meaning provided in the clause 52.204–25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

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 pursuant to 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)).

Service-disabled veteran-owned small business (SDVOSB) concern means a small business concern—

(1)(i) Not less than 51 percent of which is owned and controlled 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; and

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

(2) A small business concern eligible under the SDVOSB Program in accordance with 13 CFR part 128 (see subpart 19.14).

(3) *Service-disabled veteran*, as used in this definition, 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), and who is registered in the Beneficiary Identification and Records Locator Subsystem, or successor system that is maintained by the Department of Veterans Affairs' Veterans Benefits Administration, as a service-disabled veteran.

Service-disabled veteran-owned small business (SDVOSB) concern eligible under the SDVOSB Program means an SDVOSB concern that—

(1) Effective January 1, 2024, is designated in the System for Award Management (SAM) as certified by the Small Business Administration (SBA) in accordance with 13 CFR 128.300; or

(2) Has represented that it is an SDVOSB concern in SAM and submitted a complete application for certification to SBA on or before December 31, 2023.

Service-disabled veteran-owned small business (SDVOSB) Program means a program that authorizes contracting officers to limit competition, including award on a sole-source basis, to SDVOSB concerns eligible under the SDVOSB Program.

Small business concern—

(1) Means a concern, including its affiliates, that is independently owned and operated, not dominant in its field of operation, and qualified as a small business under the criteria in 13 CFR part 121 and size standards in this solicitation.

(2) *Affiliates*, as used in this definition, means business concerns, one of whom directly or indirectly controls or has the power to control the others, or a third party or parties control or have the power to control the others. In determining whether affiliation exists, consideration is given to all appropriate factors including common ownership, common management, and contractual relationships. SBA determines affiliation based on the factors set forth at 13 CFR 121.103.

Small disadvantaged business concern, consistent with 13 CFR 124.1001, means a small business concern under the size standard applicable to the acquisition, that—

(1) Is at least 51 percent unconditionally and directly owned (as defined at 13 CFR 124.105) by—

(i) One or more socially disadvantaged (as defined at 13 CFR 124.103) and economically disadvantaged (as defined at 13 CFR 124.104) individuals who are citizens of the United States; and

(ii) Each individual claiming economic disadvantage has a net worth not exceeding the threshold at 13 CFR 124.104(c)(2) after taking into account the applicable exclusions set forth at 13 CFR 124.104(c)(2); and

(2) The management and daily business operations of which are controlled (as defined at 13 CFR 124.106) by individuals, who meet the criteria in paragraphs (1)(i) and (ii) of this definition.

Subsidiary means an entity in which more than 50 percent of the entity is owned—

(1) Directly by a parent corporation; or

(2) Through another subsidiary of a parent corporation.

Successor means an entity that has replaced a predecessor by acquiring the assets and carrying out the affairs of the predecessor under a new name (often through acquisition or merger). The term “successor” does not include new offices/divisions of the same company or a company that only changes its name. The extent of the responsibility of the successor for the liabilities of the predecessor may vary, depending on State law and specific circumstances.

Veteran-owned small business concern means a small business concern—

(1) Not less than 51 percent of which is owned and controlled by one or more veterans (as defined at 38 U.S.C. 101(2)) 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 veterans; and

(2) The management and daily business operations of which are controlled by one or more veterans.

Women-owned business concern means a concern which is at least 51 percent owned by one or more women; or in the case of any publicly owned business, at least 51 percent of its stock is

owned by one or more women; and whose management and daily business operations are controlled by one or more women.

Women-owned small business concern means a small business concern—

- (1) That is at least 51 percent owned by one or more women; or, in the case of any publicly owned business, at least 51 percent of the stock of which is owned by one or more women; and
- (2) Whose management and daily business operations are controlled by one or more women.

Women-owned small business (WOSB) concern eligible under the WOSB Program (in accordance with 13 CFR part 127), means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States, and the concern is certified by SBA or an approved third-party certifier in accordance with 13 CFR 127.300.

(b)(1) Annual Representations and Certifications. Any changes provided by the Offeror in paragraph (b)(2) of this provision do not automatically change the representations and certifications in SAM.

(2) The offeror has completed the annual representations and certifications electronically in SAM accessed through <http://www.sam.gov>. After reviewing SAM information, the Offeror verifies by submission of this offer that the representations and certifications currently posted electronically at FAR 52.212–3, Offeror Representations and Certifications—Commercial Products and Commercial Services, have been entered or updated in the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard(s) applicable to the NAICS code(s) referenced for this solicitation), at the time this offer is submitted and are incorporated in this offer by reference (see FAR 4.1201), except for paragraphs .

(c) Offerors must complete the following representations when the resulting contract is for supplies to be delivered or services to be performed in the United States or its outlying areas, or when the contracting officer has applied part 19 in accordance with 19.000(b)(1)(ii). Check all that apply.

(1) *Small business concern*. The offeror represents as part of its offer that—

(i) It ☐ is, ☐ is not a small business concern; or

(ii) It ☐ is, ☐ is not a small business joint venture that complies with the requirements of 13 CFR 121.103(h) and 13 CFR 125.8(a) and (b). [*The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.*]

(2) *Veteran-owned small business concern*. [*Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.*] The offeror represents as part of its offer that it ☐ is, ☐ is not a veteran-owned small business concern.

(3) *SDVOSB concern.* [Complete only if the offeror represented itself as a veteran-owned small business concern in paragraph (c)(2) of this provision.] The offeror represents that it [] is, [] is not an SDVOSB concern.

(4) *SDVOSB concern joint venture eligible under the SDVOSB Program.* The offeror represents that it [] is, [] is not an SDVOSB joint venture eligible under the SDVOSB Program that complies with the requirements of 13 CFR 128.402. [Complete only if the offeror represented itself as an SDVOSB concern in paragraph (c)(3) of this provision.] [The offeror shall enter the name and unique entity identifier of each party to the joint venture: ____.]

(5) *Small disadvantaged business concern.* [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents that it [] is, [] is not a small disadvantaged business concern as defined in 13 CFR 124.1001.

(6) *Women-owned small business concern.* [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents that it [] is, [] is not a women-owned small business concern.

(7) *WOSB joint venture eligible under the WOSB Program.* [Complete only if the offeror represented itself as a women-owned small business concern in paragraph (c)(5) of this provision.] The offeror represents that it [] is, [] is not a joint venture that complies with the requirements of 13 CFR 127.506(a) through (c). [The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.]

(8) *Economically disadvantaged women-owned small business (EDWOSB) joint venture.* The offeror represents that it [] is, [] is not a joint venture that complies with the requirements of 13 CFR part 127.506(a) through (c). [The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.]

Note to Paragraphs (c)(9) and (10): Complete paragraphs (c)(9) and (10) only if this solicitation is expected to exceed the simplified acquisition threshold.

(9) *Women-owned business concern (other than small business concern).* [Complete only if the offeror is a women-owned business concern and did not represent itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents that it [] is a women-owned business concern.

(10) *Tie bid priority for labor surplus area concerns.* If this is an invitation for bid, small business offerors may identify the labor surplus areas in which costs to be incurred on account of manufacturing or production (by offeror or first-tier subcontractors) amount to more than 50 percent of the contract price:

(11) *HUBZone small business concern.* [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents, as part of its offer, that—

(i) It [] is, [] is not a HUBZone small business concern listed, on the date of this representation, as having been certified by SBA as a HUBZone small business concern in the

Dynamic Small Business Search and SAM, and will attempt to maintain an employment rate of HUBZone residents of 35 percent of its employees during performance of a HUBZone contract (see 13 CFR 126.200(e)(1)); and

(ii) It [] is, [] is not a HUBZone joint venture that complies with the requirements of 13 CFR Part 126.616(a) through (c). [*The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.*] Each HUBZone small business concern participating in the HUBZone joint venture shall provide representation of its HUBZone status.

(d) [Reserved]

(e) *Certification Regarding Payments to Influence Federal Transactions* (31 U.S.C. 1352). (Applies only if the contract is expected to exceed \$200,000.) By submission of its offer, the offeror certifies to the best of its knowledge and belief that no Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress or an employee of a Member of Congress on his or her behalf in connection with the award of any resultant contract. If any registrants under the Lobbying Disclosure Act of 1995 have made a lobbying contact on behalf of the offeror with respect to this contract, the offeror shall complete and submit, with its offer, OMB Standard Form LLL, Disclosure of Lobbying Activities, to provide the name of the registrants. The offeror need not report regularly employed officers or employees of the offeror to whom payments of reasonable compensation were made.

(f) *Buy American Certificate*. (Applies only if the clause at Federal Acquisition Regulation (FAR) 52.225-1, Buy American—Supplies, is included in this solicitation.)

(1)(i) The Offeror certifies that each end product, except those listed in paragraph (f)(2) of this provision, is a domestic end product and that each domestic end product listed in paragraph (f)(3) of this provision contains a critical component.

(ii) The Offeror shall list as foreign end products those end products manufactured in the United States that do not qualify as domestic end products. For those foreign end products that do not consist wholly or predominantly of iron or steel or a combination of both, the Offeror shall also indicate whether these foreign end products exceed 55 percent domestic content, except for those that are COTS items. If the percentage of the domestic content is unknown, select “no”.

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

(iv) The terms “commercially available off-the-shelf (COTS) item,” “critical component,” “domestic end product,” “end product,” “foreign end product,” and “United States” are defined in the clause of this solicitation entitled “Buy American—Supplies.”

(2) Foreign End Products:

Line item No.	Country of origin	Exceeds 55% domestic content (yes/no)

[List as necessary]

(3) Domestic end products containing a critical component: Line Item No. _____

[List as necessary]

(4) The Government will evaluate offers in accordance with the policies and procedures of FAR part 25.

(g)(1) *Buy American—Free Trade Agreements—Israeli Trade Act Certificate*. (Applies only if the clause at FAR 52.225-3, Buy American—Free Trade Agreements—Israeli Trade Act, is included in this solicitation.)

(i)(A) The Offeror certifies that each end product, except those listed in paragraph (g)(1)(ii) or (iii) of this provision, is a domestic end product and that each domestic end product listed in paragraph (g)(1)(iv) of this provision contains a critical component.

(B) 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.”

(ii) The Offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahraini, Moroccan, Omani, Panamanian, or Peruvian end products) or Israeli end products as defined in the clause of this solicitation entitled “Buy American—Free Trade Agreements—Israeli Trade Act.”

Free Trade Agreement Country End Products (Other than Bahraini, Moroccan, Omani, Panamanian, or Peruvian End Products) or Israeli End Products:

Line item No.	Country of origin

[List as necessary]

(iii) The Offeror shall list those supplies that are foreign end products (other than those listed in paragraph (g)(1)(ii) of this provision) as defined in the clause of this solicitation entitled “Buy American—Free Trade Agreements—Israeli Trade Act.” The Offeror shall list as other foreign end products those end products manufactured in the United States that do not qualify as domestic end products. For those foreign end products that do not consist wholly or predominantly of iron or steel or a combination of both, the Offeror shall also indicate whether

these foreign end products exceed 55 percent domestic content, except for those that are COTS items. If the percentage of the domestic content is unknown, select “no”.

Other Foreign End Products:

Line item No.	Country of origin	Exceeds 55% domestic content (yes/no)

[List as necessary]

(iv) The Offeror shall list the line item numbers of domestic end products that contain a critical component (see FAR 25.105). Line Item No. _____

[List as necessary]

(v) The Government will evaluate offers in accordance with the policies and procedures of FAR part 25.

(2) *Buy American—Free Trade Agreements—Israeli Trade Act Certificate, Alternate II.* If *Alternate II* to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g)(1)(ii) 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.	Country of origin

[List as necessary]

(3) *Buy American—Free Trade Agreements—Israeli Trade Act Certificate, Alternate III.* If *Alternate III* to the clause at 52.225-3 is included in this solicitation, substitute the following paragraphs (g)(1)(i)(B) and (g)(1)(ii) for paragraphs (g)(1)(i)(B) and (g)(1)(ii) of the basic provision:

(g)(1)(i)(B) The terms “Korean 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.”

(g)(1)(ii) The Offeror certifies that the following supplies are Korean end products or Israeli end products as defined in the clause of this solicitation entitled “Buy American—Free Trade Agreements—Israeli Trade Act”:

Korean End Products or Israeli End Products:

Line item No.	Country of origin

[List as necessary]

(4) *Trade Agreements Certificate.* (Applies only if the clause at FAR 52.225-5, Trade Agreements, is included in this solicitation.)

(i) The offeror certifies that each end product, except those listed in paragraph (g)(4)(ii) of this provision, is a U.S.-made or designated country end product, as defined in the clause of this solicitation entitled “Trade Agreements”.

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

Other End Products:

Line item No.	Country of origin

[List as necessary]

(iii) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25. 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 such products are insufficient to fulfill the requirements of the solicitation.

(h) *Certification Regarding Responsibility Matters* (Executive Order 12689). (Applies only if the contract value is expected to exceed the simplified acquisition threshold.) The offeror certifies, to the best of its knowledge and belief, that the offeror and/or any of its principals—

(1) ☐ Are, ☐ are not presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency;

(2) ☐ Have, ☐ have not, within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a Federal, state or local government contract or subcontract; violation of Federal or state antitrust statutes relating to the submission of offers; or Commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating Federal criminal tax laws, or receiving stolen property;

(3) ☐ Are, ☐ are not presently indicted for, or otherwise criminally or civilly charged by a Government entity with, commission of any of these offenses enumerated in paragraph (h)(2) of this clause; and

(4) ☐ Have, ☐ have not, within a three-year period preceding this offer, been notified of any delinquent Federal taxes in an amount that exceeds the threshold at 9.104–5(a)(2) for which the liability remains unsatisfied.

(i) Taxes are considered delinquent if both of the following criteria apply:

(A) *The tax liability is finally determined.* The liability is finally determined if it has been assessed. A liability is not finally determined if there is a pending administrative or judicial challenge. In the case of a judicial challenge to the liability, the liability is not finally determined until all judicial appeal rights have been exhausted.

(B) *The taxpayer is delinquent in making payment.* A taxpayer is delinquent if the taxpayer has failed to pay the tax liability when full payment was due and required. A taxpayer is not delinquent in cases where enforced collection action is precluded.

(ii) *Examples.*

(A) The taxpayer has received a statutory notice of deficiency, under I.R.C. Sec. 6212, which entitles the taxpayer to seek Tax Court review of a proposed tax deficiency. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek Tax Court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.

(B) The IRS has filed a notice of Federal tax lien with respect to an assessed tax liability, and the taxpayer has been issued a notice under I.R.C. Sec. 6320 entitling the taxpayer to request a hearing with the IRS Office of Appeals contesting the lien filing, and to further appeal to the Tax Court if the IRS determines to sustain the lien filing. In the course of the hearing, the taxpayer is entitled to contest the underlying tax liability because the taxpayer has had no prior opportunity to contest the liability. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek tax court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.

(C) The taxpayer has entered into an installment agreement pursuant to I.R.C. Sec. 6159. The taxpayer is making timely payments and is in full compliance with the agreement terms. The taxpayer is not delinquent because the taxpayer is not currently required to make full payment.

(D) The taxpayer has filed for bankruptcy protection. The taxpayer is not delinquent because enforced collection action is stayed under 11 U.S.C. 362 (the Bankruptcy Code).

(i) *Certification Regarding Knowledge of Child Labor for Listed End Products (Executive Order 13126).*

(1) *Listed end products.*

Listed end product	Listed countries of origin

(2) *Certification. [If the Contracting Officer has identified end products and countries of origin in paragraph (i)(1) of this provision, then the offeror must certify to either (i)(2)(i) or (i)(2)(ii) by checking the appropriate block.]*

☐ (i) The offeror will not supply any end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product.

☐ (ii) The offeror may supply an end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product. The offeror certifies that it has made a good faith effort to determine whether forced or indentured child labor was used to mine, produce, or manufacture any such end product furnished under this contract. On the basis of those efforts, the offeror certifies that it is not aware of any such use of child labor.

(j) *Place of manufacture.* (Does not apply unless the solicitation is predominantly for the acquisition of manufactured end products.) For statistical purposes only, the offeror shall indicate whether the place of manufacture of the end products it expects to provide in response to this solicitation is predominantly—

(1) ☐ In the United States (Check this box if the total anticipated price of offered end products manufactured in the United States exceeds the total anticipated price of offered end products manufactured outside the United States); or

(2) ☐ Outside the United States.

(k) *Certificates regarding exemptions from the application of the Service Contract Labor Standards.* (Certification by the offeror as to its compliance with respect to the contract also constitutes its certification as to compliance by its subcontractor if it subcontracts out the exempt

services.) [The contracting officer is to check a box to indicate if paragraph (k)(1) or (k)(2) applies.]

☐ (1) Maintenance, calibration, or repair of certain equipment as described in FAR 22.1003-4(c)(1). The offeror ☐ does ☐ does not certify that—

(i) The items of equipment to be serviced under this contract are used regularly for other than Governmental purposes and are sold or traded by the offeror (or subcontractor in the case of an exempt subcontract) in substantial quantities to the general public in the course of normal business operations;

(ii) The services will be furnished at prices which are, or are based on, established catalog or market prices (see FAR 22.1003-4(c)(2)(ii)) for the maintenance, calibration, or repair of such equipment; and

(iii) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract will be the same as that used for these employees and equivalent employees servicing the same equipment of commercial customers.

☐ (2) Certain services as described in FAR 22.1003-4(d)(1). The offeror ☐ does ☐ does not certify that—

(i) The services under the contract are offered and sold regularly to non-Governmental customers, and are provided by the offeror (or subcontractor in the case of an exempt subcontract) to the general public in substantial quantities in the course of normal business operations;

(ii) The contract services will be furnished at prices that are, or are based on, established catalog or market prices (see FAR 22.1003-4(d)(2)(iii));

(iii) Each service employee who will perform the services under the contract will spend only a small portion of his or her time (a monthly average of less than 20 percent of the available hours on an annualized basis, or less than 20 percent of available hours during the contract period if the contract period is less than a month) servicing the Government contract; and

(iv) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract is the same as that used for these employees and equivalent employees servicing commercial customers.

(3) If paragraph (k)(1) or (k)(2) of this clause applies—

(i) If the offeror does not certify to the conditions in paragraph (k)(1) or (k)(2) and the Contracting Officer did not attach a Service Contract Labor Standards wage determination to the solicitation, the offeror shall notify the Contracting Officer as soon as possible; and

(ii) The Contracting Officer may not make an award to the offeror if the offeror fails to execute the certification in paragraph (k)(1) or (k)(2) of this clause or to contact the Contracting Officer as required in paragraph (k)(3)(i) of this clause.

(l) *Taxpayer Identification Number (TIN)* (26 U.S.C. 6109, 31 U.S.C. 7701). (Not applicable if the offeror is required to provide this information to SAM to be eligible for award.)

(1) All offerors must submit the information required in paragraphs (l)(3) through (l)(5) of this provision to comply with debt collection requirements of 31 U.S.C. 7701(c) and 3325(d), reporting requirements of 26 U.S.C. 6041, 6041A, and 6050M, and implementing regulations issued by the Internal Revenue Service (IRS).

(2) The TIN may be used by the Government to collect and report on any delinquent amounts arising out of the offeror's relationship with the Government (31 U.S.C. 7701(c)(3)). If the resulting contract is subject to the payment reporting requirements described in FAR 4.904, the TIN provided hereunder may be matched with IRS records to verify the accuracy of the offeror's TIN.

(3) *Taxpayer Identification Number (TIN).*

☐ TIN: _____.

☐ TIN has been applied for.

☐ TIN is not required because:

☐ Offeror is a nonresident alien, foreign corporation, or foreign partnership that does not have income effectively connected with the conduct of a trade or business in the United States and does not have an office or place of business or a fiscal paying agent in the United States;

☐ Offeror is an agency or instrumentality of a foreign government;

☐ Offeror is an agency or instrumentality of the Federal Government.

(4) *Type of organization.*

☐ Sole proprietorship;

☐ Partnership;

☐ Corporate entity (not tax-exempt);

☐ Corporate entity (tax-exempt);

☐ Government entity (Federal, State, or local);

☐ Foreign government;

☐ International organization per 26 CFR 1.6049-4;

☐ Other _____.

(5) *Common parent.*

☐ Offeror is not owned or controlled by a common parent;

☐ Name and TIN of common parent:

Name _____.

TIN _____.

(m) *Restricted business operations in Sudan.* By submission of its offer, the offeror certifies that the offeror does not conduct any restricted business operations in Sudan.

(n) *Prohibition on Contracting with Inverted Domestic Corporations.*

(1) Government agencies are not permitted to use appropriated (or otherwise made available) funds for contracts with either an inverted domestic corporation, or a subsidiary of an inverted domestic corporation, unless the exception at 9.108-2(b) applies or the requirement is waived in accordance with the procedures at 9.108-4.

(2) *Representation.* The Offeror represents that—

(i) It [] is, [] is not an inverted domestic corporation; and

(ii) It [] is, [] is not a subsidiary of an inverted domestic corporation.

(o) *Prohibition on contracting with entities engaging in certain activities or transactions relating to Iran.*

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

(2) *Representation and certifications.* Unless a waiver is granted or an exception applies as provided in paragraph (o)(3) of this provision, by submission of its offer, the offeror—

(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 owned or controlled by the offeror, does not engage in any activities for which sanctions may be imposed under section 5 of the Iran Sanctions Act; and

(iii) Certifies that the offeror, and any person owned or controlled by the offeror, does not knowingly engage in any transaction that exceeds the threshold at FAR 25.703–2(a)(2) 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>).

(3) The representation and certification requirements of paragraph (o)(2) of this provision do not apply if—

(i) This solicitation includes a trade agreements certification (e.g., 52.212–3(g) or a comparable agency provision); and

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

(p) *Ownership or Control of Offeror.* (Applies in all solicitations when there is a requirement to be registered in SAM or a requirement to have a unique entity identifier in the solicitation).

(1) The Offeror represents that it ☐ has or ☐ does not have an immediate owner. If the Offeror has more than one immediate owner (such as a joint venture), then the Offeror shall respond to paragraph (2) and if applicable, paragraph (3) of this provision for each participant in the joint venture.

(2) If the Offeror indicates “has” in paragraph (p)(1) of this provision, enter the following information:

Immediate owner CAGE code: _____.

Immediate owner legal name: _____.

(Do not use a “doing business as” name)

Is the immediate owner owned or controlled by another entity: ☐ Yes or ☐ No.

(3) If the Offeror indicates “yes” in paragraph (p)(2) of this provision, indicating that the immediate owner is owned or controlled by another entity, then enter the following information:

Highest-level owner CAGE code: _____.

Highest-level owner legal name: _____.

(Do not use a “doing business as” name)

(q) *Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law.*

(1) As required by sections 744 and 745 of Division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235), and similar provisions, if contained in subsequent appropriations acts, The Government will not enter into a contract with any corporation that—

(i) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless an agency has considered suspension or debarment of the corporation and made a determination that suspension or debarment is not necessary to protect the interests of the Government; or

(ii) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.

(2) The Offeror represents that—

(i) It is ☐ is not ☐ a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have

lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability; and

(ii) It is ☐ is not ☐ a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.

(r) *Predecessor of Offeror*. (Applies in all solicitations that include the provision at 52.204-16, Commercial and Government Entity Code Reporting.)

(1) The Offeror represents that it ☐ is or ☐ is not a successor to a predecessor that held a Federal contract or grant within the last three years.

(2) If the Offeror has indicated “is” in paragraph (r)(1) of this provision, enter the following information for all predecessors that held a Federal contract or grant within the last three years (if more than one predecessor, list in reverse chronological order):

Predecessor CAGE code: ____ (or mark “Unknown”).

Predecessor legal name: ____.

(Do not use a “doing business as” name).

(s) [Reserved]

(t) [Reserved]

(u)(1) In accordance with section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions), Government agencies are not permitted to use appropriated (or otherwise made available) funds for contracts with an entity that requires employees or subcontractors of such entity seeking to report waste, fraud, or abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting such waste, fraud, or abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.

(2) The prohibition in paragraph (u)(1) of this provision does not contravene requirements applicable to Standard Form 312 (Classified Information Nondisclosure Agreement), Form 4414 (Sensitive Compartmented Information Nondisclosure Agreement), or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(3) Representation. By submission of its offer, the Offeror represents that it will not require its employees or subcontractors to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting waste, fraud, or abuse related to the performance of a Government contract to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information (e.g., agency Office of the Inspector General).

(v) *Covered Telecommunications Equipment or Services—Representation*. Section 889(a)(1)(A) and section 889(a)(1)(B) of [Public Law 115-232](#).

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

(2) The Offeror represents that—

(i) It [] does, [] does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(ii) After conducting a reasonable inquiry for purposes of this representation, that it [] does, [] does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services.

(End of Provision)

E.5 52.219-1 SMALL BUSINESS PROGRAM REPRESENTATIONS (NOV 2025) (DEVIATION)

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

Economically disadvantaged women-owned small business (EDWOSB) concern means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States and who are economically disadvantaged in accordance with 13 CFR part 127, and the concern is certified by SBA or an approved third-party certifier in accordance with 13 CFR 127.300. It automatically qualifies as a women-owned small business concern eligible under the WOSB Program.

HUBZone small business concern means a small business concern that meets the requirements described in 13 CFR 126.200, is certified by the Small Business Administration (SBA) and designated by SBA as a HUBZone small business concern in the Small Business Search (SBS) (13 CFR 126.103).

Service-disabled veteran-owned small business (SDVOSB) concern eligible under the SDVOSB Program means an SDVOSB concern that is designated in the System for Award Management (SAM) as certified by the Small Business Administration (SBA) in accordance with 13 CFR 128.300.

Small business concern—

(1) Means a concern, including its affiliates, that is independently owned and operated, not dominant in its field of operation, and qualified as a small business under the criteria in 13 CFR part 121 and the size standard in paragraph (b) of this provision.

(2) *Affiliates*, as used in this definition, means business concerns, one of whom directly or indirectly controls or has the power to control the others, or a third party or parties control or have the power to control the others. In determining whether affiliation exists, consideration is given to all appropriate factors including common ownership, common management, and

contractual relationships. SBA determines affiliation based on the factors set forth at 13 CFR 121.103.

Small disadvantaged business concern, means a small business concern that-

(1) Is at least 51 percent unconditionally and directly owned (as defined at 13 CFR 124.105) by one or more socially disadvantaged (as defined at 13 CFR 124.103) and economically disadvantaged (as defined at 13 CFR 124.104) individuals who are citizens of the United States, and

(2) The management and daily business operations of which are controlled (as defined at 13 CFR 124.106) by individuals who meet the criteria in paragraph (1) of this definition.

Women-owned small business (WOSB) concern eligible under the WOSB Program (in accordance with 13 CFR part 127) means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States, and the concern is certified by SBA or an approved third-party certifier in accordance with 13 CFR 127.300.

(b)(1) The North American Industry Classification System (NAICS) code for this acquisition is 561621.

(2) The small business size standard is \$25 Million.

(3) The small business size standard for a concern that submits an offer, other than on a construction or service acquisition, but proposes to furnish an end item that it did not itself manufacture, process, or produce (*i.e.*, nonmanufacturer), is 500 employees, or 150 employees for information technology value-added resellers under NAICS code 541519, if the acquisition—

(i) Is set aside for small business and has a value above the simplified acquisition threshold;

(ii) Uses the HUBZone price evaluation preference regardless of dollar value, unless the offeror waives the price evaluation preference; or

(iii) Is an 8(a), HUBZone, service-disabled veteran-owned, economically disadvantaged women-owned, or women-owned small business set-aside or sole-source award regardless of dollar value.

(c) *Representations.*

(1) The offeror represents as part of its offer that—

(i) It [] is, [] is not a small business concern; or

(ii) It [] is, [] is not a small business joint venture that complies with the requirements of 13 CFR 121.103(h) and 13 CFR 125.8(a) and (b). [*The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.*]

(2) *[Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.]* The offeror represents that it ☐ is, ☐ is not, a women-owned small disadvantaged business concern.

(3) *Women-owned small business (WOSB) joint venture eligible under the WOSB Program.* The offeror represents as part of its offer that it ☐ is, ☐ is not a joint venture that complies with the requirements of 13 CFR 127.506(a) through (c). *[The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.]*

(4) *Economically disadvantaged women-owned small business (EDWOSB) joint venture.* The offeror represents as part of its offer that it ☐ is, ☐ is not a joint venture that complies with the requirements of 13 CFR 127.506(a) through (c). *[The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.]*

(5) *SDVOSB joint venture eligible under the SDVOSB Program. [Complete only if the offeror is certified as a SDVOSB concern.]* The offeror represents as part of its offer that it ☐ is, ☐ is not a SDVOSB joint venture eligible under the SDVOSB Program that complies with the requirements of 13 CFR 128.402. *[The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.]*

(6) *HUBZone joint venture eligible under the HUBZone Program. [Complete only if the offeror is a HUBZone small business concern.]* The offeror represents, as part of its offer, that it ☐ is, ☐ is not a HUBZone joint venture that complies with the requirements of 13 CFR 126.616(a) through (c). *[The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.]* Each HUBZone small business concern participating in the HUBZone joint venture must be certified as a HUBZone concern.

(d) *Notice.*

Under 15 U.S.C. 645(d), any person who misrepresents a firm's status as a business concern that is small, HUBZone small, small disadvantaged, service-disabled veteran-owned small, economically disadvantaged women-owned small, or women-owned small eligible under the WOSB Program in order to obtain a contract to be awarded under the preference programs established pursuant to section 8, 9, 15, 31, and 36 of the Small Business Act or any other provision of Federal law that specifically references section 8(d) for a definition of program eligibility, will be—

- (1) Punished by imposition of fine, imprisonment, or both;
- (2) Subject to administrative remedies, including suspension and debarment; and
- (3) Ineligible for participation in programs conducted under the authority of the Act.

(End of Provision)

E.6 52.233-2 SERVICE OF PROTEST (SEP 2006)

Protests, as defined in section 33.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government

Accountability Office (GAO), shall be served on the Contracting Officer (addressed as follows) by obtaining written and dated acknowledgment of receipt from:

Department of Veterans Affairs

Network Contracting Office 4
Hand-Carried Address:

Services 2

1010 Delafield Rd.
Pittsburgh PA 15215
Mailing Address:

Services 2

1010 Delafield Rd.
Pittsburgh PA 15215

(b) The copy of any protest shall be received in the office designated above within one day of filing a protest with the GAO.

(End of Provision)

E.7 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.8 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)

<u>FAR Number</u>	<u>Title</u>	<u>Date</u>
52.203-11	CERTIFICATION AND DISCLOSURE REGARDING PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS	SEP 2024
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
52.229-11	TAX ON CERTAIN FOREIGN PROCUREMENTS—NOTICE AND REPRESENTATION	JUN 2020
852.233-70	PROTEST CONTENT/ALTERNATIVE DISPUTE RESOLUTION	OCT 2018
852.233-71	ALTERNATE PROTEST PROCEDURE	OCT 2018
852.239-70	SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES	FEB 2023
852.239-71	INFORMATION SYSTEM SECURITY PLAN AND ACCREDITATION	FEB 2023
852.239-75	INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY NOTICE	FEB 2023

E.9 52.252-5 AUTHORIZED DEVIATIONS IN PROVISIONS (NOV 2020)

(a) The use in this solicitation of any Federal Acquisition Regulation (48 CFR Chapter 1) provision with an authorized deviation is indicated by the addition of “(DEVIATION)” after the date of the provision.

(b) The use in this solicitation of any VAAR Acquisition Regulation (48 CFR Chapter FEDERAL ACQUISITION REGULATION (48 CFR Chapter 1)) provision with an authorized deviation is indicated by the addition of “(DEVIATION)” after the name of the regulation.

(End of Provision)

End of Document