SOLICITATION, OFFER, AND AWARD

1. This Contract is a Rated Order under the Defense Priorities and Allocations System (DPAS) - Code of Federal Regulations - at 15 CFR 700.

RATING | PAGE 1 OF PAGES 121

2. CONTRACT NUMBER	3. SOLICITATION NUMBER	4. TYPE OF SOLICITATION	5. DATE ISSUED	6. REQUISITION/PURCHASE NUMBER
	70CDCR26R00000021	☐ SEALED BID (IFB) INVITATION FOR BID ☒ NEGOTIATED (RFP) REQUEST FOR PROPOSAL	07/27/2026	

7. ISSUED BY CODE 70CDCR
DETENTION COMPLIANCE AND REMOVALS
ICE Office of Acquisition Management
500 12th St SW
WASHINGTON DC 20024

8. ADDRESS OFFER TO *(If other than item 7)*
Shane.Crowl@ice.dhs.gov
CC: Brittany.Tobias@ice.dhs.gov

NOTE: In sealed bid solicitations "offer" and "offeror" mean "bid" and "bidder".

SOLICITATION

9. Sealed offers in original and 1 copies for furnishings the supplies or services in the Schedule will be received at the place specified in item 8, or if hand carried, in the depository located in _____ until 1700 ES *(Hour)* local time 08/10/2026 *(Date)*

CAUTION - LATE Submissions, Modifications, and Withdrawals: See Section L, Provision Number 52.214-7 or 52.215-1. All offers are subject to all terms and conditions contained in this solicitation.

10. FOR INFORMATION CALL:	A. NAME	B. TELEPHONE *(NO COLLECT CALLS)* AREA CODE	NUMBER	EXTENSION	C. EMAIL ADDRESS
	SHANE CROWL				shane.crowl@ice.dhs.gov

11. TABLE OF CONTENTS

(X)	SECTION	DESCRIPTION	PAGE(S)	(X)	SECTION	DESCRIPTION	PAGE(S)
		PART I - THE SCHEDULE				*PART II - CONTRACT CLAUSES*	
☒	A	SOLICITATION/CONTRACT FORM	1	☒	I	CONTRACT CLAUSES	27
☒	B	SUPPLIES OR SERVICES AND PRICES/COSTS	3			*PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS*	
☒	C	DESCRIPTION/SPECIFICATIONS/WORK STATEMENT	4	☒	J	LIST OF ATTACHMENTS	68
☒	D	PACKAGING AND MARKING	5			*PART IV - REPRESENTATIONS AND INSTRUCTIONS*	
☒	E	INSPECTION AND ACCEPTANCE	6	☒	K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	69
☒	F	DELIVERIES OR PERFORMANCE	7				
☒	G	CONTRACT ADMINISTRATION DATA	8	☒	L	INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS	105
☒	H	SPECIAL CONTRACT REQUIREMENTS	9	☒	M	EVALUATION FACTORS FOR AWARD	115

OFFER *(Must be fully completed by offeror)*

NOTE: Item 12 does not apply if the solicitation includes the provisions at 52.214-16, Minimum Bid Acceptance Period.

12. In compliance with the above, the undersigned agrees, if this offer is accepted within 0 calendar days *(60 calendar days unless a different period is inserted by the offeror)* from the date for receipt of offers specified above, to furnish any or all items upon which prices are offered at the set opposite each item, delivered at the designated point(s), within the time specified in the schedule.

13. DISCOUNT FOR PROMPT PAYMENT *(See Section I, Clause Number 52.232-8)*	10 CALENDAR DAYS (%)	20 CALENDAR DAYS (%)	30 CALENDAR DAYS (%)	CALENDAR DAYS (%)

14. ACKNOWLEDGMENT OF AMENDMENTS *(The offeror acknowledges receipt of amendments to the SOLICITATION for offerors and related documents numbered and dated):*	AMENDMENT NUMBER	DATE	AMENDMENT NUMBER	DATE

15A. NAME AND ADDRESS OF OFFEROR
CODE _____ FACILITY _____

16. NAME AND THE TITLE OF PERSON AUTHORIZED TO SIGN OFFER *(Type or print)*

15B. TELEPHONE NUMBER AREA CODE	NUMBER	EXTENSION	☐ 15C. CHECK IF REMITTANCE ADDRESS IS DIFFERENT FROM ABOVE - ENTER SUCH ADDRESS IN SCHEDULE.	17. SIGNATURE	18. OFFER DATE

AWARD *(To be completed by Government)*

19. ACCEPTED AS TO ITEMS NUMBERED	20. AMOUNT	21. ACCOUNTING AND APPROPRIATION

22. AUTHORITY FOR USING OTHER THAN FULL OPEN COMPETITION UNDER THE UNITED STATES CODE AT:
☐ 10 U.S.C. 3204(a) ( ) ☐ 41 U.S.C. 3304(a) ( )

23. SUBMIT INVOICES TO ADDRESS SHOWN IN *(4 copies unless otherwise specified)* | ITEM

24. ADMINISTERED BY *(If other than Item 7)* CODE _____

25. PAYMENT WILL BE MADE BY CODE _____

26. NAME OF CONTRACTING OFFICER *(Type or print)*	27. UNITED STATES OF AMERICA *(Signature of Contracting Officer)*	28. AWARD DATE
SHANE CROWL		

IMPORTANT - Award will be made on this Form, or on Standard Form 26, or by other authorized official written notice.

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Solicitation for 287(g) Texas Transportation in accordance with sections A-M of this Request for Proposal (RFP), including Attachments (See Section J).				

SECTION B:
SUPPLIES OR SERVICES AND PRICES/COSTS

B.1. GENERAL

The contractor shall provide all management, supervision, personnel, training, certifications, vehicles, facilities, equipment, materials, supplies, and quality control necessary to perform the safe, secure, humane, and expeditious armed ground transportation services identified in the Performance Work Statement (PWS) for individuals arrested under the 287(g) Program throughout the State of Texas, including transport to ICE designated locations in Texas, Oklahoma and New Mexico and operation of a centralized dispatch center and secure web portal.

B.2. CONTRACT TYPE

This is a Firm-Fixed-Price (FFP) contract.

B.3. CLIN STRUCTURE

See Attachment-02 Pricing Template for anticipated CLIN structure.

Note: The government may establish a single CLIN for transportation services (X001), and a single CLIN for dispatch services (X002), given the number of locations required. In this event, the government will incorporate the offerors price sheet as an attachment to the resultant contract award.

[END OF SECTION B]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION C:
DESCRIPTION/SPECIFICATIONS

C.1. PERFORMANCE WORK STATEMENT (PWS)

The PWS is attached to this solicitation; see Attachment 01 – Performance Work Statement.

[END OF SECTION C]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION D:
PACKING AND MARKING

D.1. PACKING AND MARKING

No packing or marking requirements are applicable to this requirement.

[END OF SECTION D]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION E:
INSPECTION AND ACCEPTANCE

E.1. CLAUSES AND/OR PROVISIONS INCORPORATED BY REFERENCE

The following clauses are incorporated by reference:

Number	Title	Date
52.204-7	System for Award Management	Nov 2024
52.212-4	Contract Terms and Conditions – Commercial Products and Commercial Services (DEVIATION 25-21)	

E.2. INSPECTION AND ACCEPTANCE

The government will conduct inspection and acceptance for all rendered services including deliverables in accordance with FAR 52.212-4 (DEVIATION 25-21). See:

Attachment 01 – Performance Work Statement

E.3. CONTRACTOR PERFORMANCE ASSESSMENT REPORTING SYSTEM (CPARS)

In accordance with Federal Acquisition Regulation (FAR) Subpart 42.15, it is anticipated that past performance evaluations will be entered into CPARS, the governmentwide evaluation reporting tool for all past performance reports on contracts and orders. For more information regarding CPARS, please visit http://www.cpars.gov/.

E.4. QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

Services will be evaluated in accordance with the metrics outlined in the QASP contained within Attachment 01- Performance Work Statement.

[END OF SECTION E]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION F:
DELIVERIES OR PERFORMANCE

F.1. CLAUSES AND/OR PROVISIONS INCORPORATED BY REFERENCE

The following clauses are incorporated by reference:

Number	Title	Date
52.242-15	Stop-Work Order	Aug 1989

F.2. PERIOD OF PERFORMANCE

The anticipated period of performance will include a single base period of 12- months inclusive of a 120 day transition-in period; and Option Period One: 36 months, if exercised by the Government.

F.3. PLACE OF PERFORMANCE

Primary place of performance:

- State of Texas (all 254 counties)

Delivery locations:

- ICE facilities in Texas, Oklahoma, and New Mexico, as directed by ICE ERO.

Dispatch Center

- Contractor dispatch operations shall be located within the ICE 287(g) National Coordination Center in the greater Nashville, Tennessee area, as described in the PWS. The Government will provide space; the contractor will furnish and operate all equipment within that space.

F.4. LIST OF DELIVERABLES

For a complete list of contract deliverables and associated due dates, see:

- Attachment 01 – Performance Work Statement (PWS)

[END OF SECTION F]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION G:
CONTRACT ADMINISTRATION DATA

G.1. CONTRACT ADMINISTRATION

Notwithstanding the contractor's responsibility for management of daily of operations of the facility during the contract performance, the administration of the contract will require coordination between ICE and the contractor.

G.2. CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The following individual is designated as the COR for this requirement and is authorized by the contracting officer (CO) to perform specific contract administration functions such as inspection and acceptance of services and other functions of a technical nature:

The CORs will represent the CO in the administration of technical details within the scope of the Contract. The CORs are also responsible for the final inspection and acceptance of all Contract deliverables and reports. The CORs are not otherwise authorized to make any representations or commitments of any kind on behalf of the CO or the Government. The CORs do not have authority to alter the contractor's obligations or to change the contract specifications, price, terms or conditions. If, as a result of technical discussions, it is desirable to modify contract obligations or the specification, changes will be issued in writing and signed by the CO.

The COR will monitor contractor performance using the Quality Assurance Surveillance Plan (QASP), and will verify compliance with the performance standards, Acceptable Quality Levels (AQLs), and deliverable requirements set forth in the PWS.

G.3. INVOICE INSTRUCTIONS

The Contractor shall invoice in accordance with the PWS and any additional instructions provided in the award document (including the designated electronic invoicing system). At a minimum, invoices shall be supported by the monthly performance and reporting documentation.

[END OF SECTION G]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION H:
SPECIAL CONTRACT REQUIREMENTS

H.1. PERFORMANCE-BASED SERVICES CONTRACTING (PBSC)

Through the direction of the Office of Management and Budget (OMB), Office of Federal Procurement Policy (OFPP), performance-based contracting techniques will be applied to this contract to the "maximum extent practicable." For information about PBSC, refer to RFO 37.101.

Performance-based contracts for service must include:

a) Performance requirements that define the work in measurable, mission-related terms;
b) Performance standards (i.e., quality, quantity, timeliness) tied to the performance requirements; and
c) A Government QASP or other suitable plan that describes how the contractor's performance will be measured against the performance standards or service level agreements (SLAs).

H.2. DISCLOSURE OF INFORMATION – OFFICIAL USE ONLY

Each officer or employee of the contractor or subcontractor at any tier to whom "Official Use Only" information may be made available or disclosed, shall be notified in writing by the contractor that "Official Use Only" information disclosed to that individual can be used only for a purpose, and to the extent authorized herein, and that further disclosure of any such "Official Use Only" information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. Sections 641 and 3571. Section 641 of 18 U.S.C. provides, in pertinent part, that whoever knowingly converts to his use or the use of another, or without authority sells, conveys, or disposes of any record of the United States or whoever receives the same with the intent to convert it to his use or gain, knowing it to have been converted, shall be guilty of a crime punishable by a fine or imprisoned up to 10 years, or both.

H.3. CONTRACTOR'S INSURANCE AND FAR 52.228-10

The contractor shall maintain insurance in an amount not less than $3,000,000 to protect the contractor from claims under workman compensation acts and from any other claims for damages for personal injury, including death which may arise from operations under this contract whether such operations by the contractor itself or by any subcontractor or anyone directly or indirectly employed by either business entity. The contractor shall maintain general liability insurance: bodily injury liability coverage written on a comprehensive form of policy of at least $500,000 per occurrence is required.

Additionally, an automobile liability insurance policy providing for bodily injury and property damage liability covering automobiles operated in the United States (U.S.) shall provide coverage of at least $200,000 per person and $500,000 per occurrence for bodily injury and $20,000 per occurrence for property coverage. Certificates of such insurance shall be subject to the approval of the CO for adequacy of protection. All insurance certificates required under this contract shall provide 30 days' notice to the government of any contemplated cancellation. The contractor shall

ensure that all staff having access to alien monies and valuables are bonded in an amount sufficient to ensure reimbursement to the alien by the contractor in case of loss.

H.4. ICE INFORMATION GOVERNANCE AND PRIVACY REQUIREMENTS (JUL 2017)

In addition to FAR 52.224-1 Privacy Act Notification (APR 1984), 52.224-2 Privacy Act (APR 1984), 52.224-3 Privacy Training – Alternate I (DEVIATION), and HSAR Clauses, the following instructions must be included in their entirety in all contracts.

Limiting Access to Privacy Act and Other Sensitive Information
In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984), and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires contractor personnel to have access to information protected by the Privacy Act of 1974, the contractor is advised that the relevant DHS system of records notices (SORNs) applicable to this Privacy Act information may be found at https://www.dhs.gov/system-records-notices-sorns. Applicable SORNS of other agencies may be accessed through the agencies' websites or by searching GovInfo, available at https://www.govinfo.gov that replaced the FDsys website in December 2018. SORNs may be updated at any time.

Prohibition on Performing Work Outside a Government Facility/Network/Equipment
The contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or Workplace as a Service (WaaS) if WaaS is authorized by the Performance Work Statement Government information shall remain within the confines of authorized Government networks at all times. Except where telework is specifically authorized within this contract, the contractor shall perform all tasks described in this document at authorized Government facilities; the contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of telework authorizations.

Prior Approval Required to Hire Subcontractors
The Contractor is required to obtain the CO's approval prior to engaging in any contractual relationship (subcontractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under or relating to this contract. The Contractor (and any Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

Separation Checklist for Contractor Employees
Contractor shall complete a separation checklist before any employee or subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally identifiable information (PII), in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the contractor's facilities or systems that would permit the terminated employee's access to sensitive PII.

In the event of adverse job actions resulting in the dismissal of an employee or subcontractor employee, the contractor shall notify the Contracting Officer's Representative (COR) within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of employment or work on the contract.

As requested, contractors shall assist the ICE Point of Contact (ICE/POC), CO, or COR with completing ICE Form 50-005/Contractor Employee Separation Clearance Checklist by returning all Government-furnished property including but not limited to computer equipment, media, credentials and passports, smart cards, mobile devices, PIV cards, calling cards, and keys and terminating access to all user accounts and systems.

Contractor's Commercial License Agreement and Government Electronic Information Rights
Except as stated in the PWS and, where applicable, the Contractor's Commercial License Agreement, the Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases) and all supporting documentation and associated metadata created as part of this contract. All deliverables (including all data and records) under the contract are the property of the U.S. Government and are considered federal records, for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

Privacy Lead Requirements
If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy documentation, the contractor shall assign or procure a privacy lead, to be listed under the PWS's required contractor personnel section. The privacy lead shall be responsible for providing adequate support to DHS to ensure DHS can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance. The Privacy Lead shall work with personnel from the program office, the ICE Privacy Unit, the Office of the Chief Information Officer, and the Records and Data Management Unit to ensure that the privacy documentation is kept on schedule, that the answers to questions in the PIA are thorough and complete, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

The Privacy Lead:

- Must have excellent writing skills, the ability to explain technology clearly for a non-technical audience, and the ability to synthesize information from a variety of sources.
- Must have excellent verbal communication and organizational skills.
- Must have experience writing PIAs. Ideally the candidate would have experience writing PIAs for DHS.
- Must be knowledgeable about the Privacy Act of 1974 and the E-Government Act of 2002.
- Must be able to work well with others.

If a Privacy Lead is already in place with the program office and the contract involves IT system builds or substantial changes that may require privacy documentation, the requirement for a separate

Private Lead specifically assigned under this contract may be waived provided the contractor agrees to have the existing Privacy Lead coordinate with and support the ICE Privacy POC to ensure privacy concerns are proactively reviewed and so ICE can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance if required. The contractor shall work with personnel from the program office, the ICE Office of Information Governance and Privacy, and the Office of the Chief Information Officer to ensure that the privacy documentation is kept on schedule, that the answers to questions in any privacy documents are thorough and complete, that all records management requirements are met, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

H.5. COMPLIANCE WITH DHS SECURITY POLICY TERMS AND CONDITIONS

All hardware, software, and services provided under this task order must be compliant with *DHS National Security Systems Policy Directive 4300B, Version 10.1, November 21, 2018' for NSS Collateral (Unclass, Secret or Top Secret Collateral)*.

H.6. ENCRYPTION COMPLIANCE TERMS AND CONDITIONS

If encryption is required, the following methods are acceptable for encrypting sensitive information:

a) FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.
b) National Security Agency (NSA) Type 2 or Type 1 encryption.
c) Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the *Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems*).

H.7. SECURITY REVIEW TERMS AND CONDITIONS

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The contractor shall afford ICE, including the organization of ICE Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer Representative (COR), and other government oversight organizations, access to the contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The contractor will contact ICE Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to ICE. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of ICE data or the function of computer system operated on behalf of ICE, and to preserve evidence of computer crime.

H.8. INTERCONNECTION SECURITY AGREEMENT (ISA) TERMS AND CONDITIONS

Interconnections between DHS/ICE and non-DHS/ICE IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be authorized at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memoranda of understanding, service level agreements or interconnection security agreements.

H.9. PERSONAL IDENTIFICATION VERIFICATION (PIV) CREDENTIAL COMPLIANCE TERMS AND CONDITIONS

a) Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

b) Procurements for software products or software developments shall be compliant by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.

c) PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.

d) If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

H.10. IN ACCORDANCE WITH FEDRAMP

1) FedRAMP IT Systems Security Requirements

a) The Federal agency will determine the security category for the cloud system in accordance with Federal Information Processing Standard 199; then, the contractor/Cloud Service Provider (CSP) shall apply the appropriate set of impact baseline controls as required in the FedRAMP Cloud Computing Security Requirements Baseline document to ensure compliance to security standards. The FedRAMP baseline controls are based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations (as amended), and also includes a set of additional controls for use within systems providing cloud services to the federal government.

b) The CSP shall maintain a security management continuous monitoring environment that meets or exceeds the requirements outlined in the latest edition of FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements.

2) FedRAMP Privacy Requirements

Contractor shall be responsible for the following privacy and security safeguards:

a) To the extent required to carry out the FedRAMP assessment and authorization process and FedRAMP continuous monitoring, to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the contractor, the contractor shall afford the Government access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.
b) If new or unanticipated threats or hazards are discovered by either the Government or the contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.
c) The contractor shall also comply with any additional FedRAMP privacy requirements.
d) The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. In accordance with the Federal Acquisitions Regulations (FAR) clause 52.239-1, contractor shall be responsible for the following privacy and security safeguards:
    i. The contractor shall not publish or disclose in any manner, without the CO's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception—Disclosure to a Consumer Agency for purposes of C&A verification.
    ii. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the contractor shall afford the Government access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours. The program of inspection shall include, but is not limited to: Authenticated and unauthenticated operating system/network vulnerability scans Authenticated and unauthenticated we b application vulnerability scans Authenticated and unauthenticated database application vulnerability scans Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools.
    iii. If new or unanticipated threats or hazards are discovered by either the Government or the contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.
    iv. If the vendor chooses to run its own automated scans or audits, results from these scans may, at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided, in full, to the Government.

3) Sensitive Information Storage

Controlled Unclassified information (CUI), data, and/or equipment will only be disclosed to

authorize personnel on a need-to-know basis. The contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST SP 800-88, Guidelines for Media Sanitization.

The disposition of all data will be at the written direction of the COR; this may include documents returned to Government control; destroyed; or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the COR.

4) Protection of Information

The contractor shall be responsible for properly protecting all information used, gathered, or developed because of work under this contract. The contractor shall also protect all Government data, equipment, etc. by treating the information as sensitive. All information about the systems gathered or created under this contract should be considered as CUI information. It is anticipated that this information will be gathered, created, and stored within the primary work location. If contractor personnel must remove any information from the primary work area they should protect it to the same extent they would their proprietary data and/or company trade secrets. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

The government will retain unrestricted rights to government data. The government retains ownership of any user created/loaded data and applications hosted on vendor’s infrastructure, as well as maintains the right to request full copies of these at any time.

The data that is processed and stored by the various applications within the network infrastructure contains financial data as well as personally identifiable information (PII). This data and PII shall be protected against unauthorized access, disclosure or modification, theft, or destruction. The contractor shall ensure that the facilities that house the network infrastructure are physically secure.

The government-owned data must be available to the Government upon request within one business day or within the timeframe specified otherwise and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the government.

No data shall be released by the contractor without the consent of the Government in writing. All requests for release must be submitted in writing to the COR/CO.

5) Security Classification

The preparation of the deliverables in this contract will be completed at a Sensitive but Unclassified level unless a higher level is specified.

6) Confidentiality and Nondisclosure

The preliminary and final deliverables and all associated working papers and other material deemed relevant by the agency that have been generated by the contractor in the performance of this contract, are the property of the U.S. Government, and must be submitted to the COR at the conclusion of the contract. The U.S. Government has unlimited data rights to all deliverables and associated working papers and materials in accordance with FAR 52.227-1, 52.227-2, 52.227-3, 52.227-11, 52.227-14, 52.227-16.

All documents produced for this project are the property of the U.S. Government and cannot be reproduced or retained by the contractor. All appropriate project documentation will be given to the agency during and at the end of this contract. The contractor shall not release any information without the written consent of the CO.

Personnel working on any of the tasks described may, at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

7) Disclosure of Information

Any information made available to the contractor by the Government shall be used only for carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the contractor or the contractor's responsible employees. Each officer or employee of the contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

8) FedRAMP Security Requirements Overview:

a) The minimum requirements for low and moderate impact cloud systems are contained within the FedRAMP Cloud Computing Security Requirements Baseline. The contractor and Federal Government Agency share responsibility to ensure compliance with security requirements.
b) The implementation of a new Federal Government cloud system requires a formal process, known as Assessment and Authorization, which provides guidelines for performing the assessment.
c) FedRAMP requires cloud service providers to utilize a Third-Party Assessment Organization (3PAO) to perform an assessment of the cloud service provider's security controls to determine the extent to which security controls are implemented correctly,

operate as intended, and produce the desired outcome with respect to meeting security requirements.

d) The FedRAMP PMO security staff will be available for consultation during the process. Both the FedRAMP PMO staff and JAB will review the results before issuing a Provisional Authorization decision. The Government reserves the right to verify the infrastructure and security test results before issuing an Authorization decision.
e) Federal agencies will be able to leverage the provisional Authorization granted by FedRAMP and any documentation prepared by the contractor to issue their own authority to operate.
f) The vendor is advised to review the FedRAMP guidance documents (see References below) to determine the level of effort that will be necessary to complete the requirements. All FedRAMP documents and templates are available at http://FedRAMP.gov.

9) FedRAMP Security Compliance Requirements

The contractor shall implement the controls contained within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements for low and moderate impact system (as defined in FIPS 199). These documents define requirements for compliance to meet minimum Federal information security and privacy requirements for both low and moderate impact systems. While the FedRAMP baseline controls are based on NIST SP 800-53, Revision 4. The contractor shall generally, substantially, and in good faith follow FedRAMP guidelines and Security guidance. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

10) Required FedRAMP Policies and Regulations

The contractor shall comply with FedRAMP Security Assessment Framework – describing a general security Assessment Framework for the Federal Risk and Authorization Management Program (FedRAMP). This document details the security assessment process which must be used to achieve FedRAMP compliance. Download here:

https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf

11) Assessment and Authorization

DHS/ICE may choose to cancel the contract/award and terminate any outstanding orders if the contractor has its provisional authorization revoked and the deficiencies are greater than agency risk tolerance thresholds.

12) Assessment of the System

a) The contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on

the System's NIST Federal Information Processing Standard (FIPS) Publication 199 categorization. The contractor shall create, maintain and update the following documentation using FedRAMP requirements and templates, which are available at http://FedRAMP.gov :

- Privacy Impact Assessment (PIA)
- FedRAMP Test Procedures and Results
- Security Assessment Report (SAR)
- System Security Plan (SSP)
- IT System Contingency Plan (CP)
- IT System Contingency Plan (CP) Test Results
- POA&M Continuous Monitoring Plan (CMP)
- FedRAMP Control Tailoring Workbook
- Control Implementation Summary Table
- Results of Penetration Testing
- Software Code Review
- Interconnection Agreements/Service Level Agreements/Memorandum of Agreements.

b) Information systems must be assessed by an accredited 3PAO whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.
c) The Government reserves the right to perform penetration testing. If the Government exercises this right, the contractor shall allow Government employees (or designated third parties) to conduct security assessment activities to include control reviews in accordance with FedRAMP requirements (https://www.fedramp.gov/assets/resources/documents/CSP_Penetration_Test_Guidance.pdf). Review activities include but are not limited to scanning operating systems, web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.
d) Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the contractor's implementation as documented in the Security Assessment Report shall be tracked by the contractor for mitigation in a POA&M document. Depending on the severity of the gaps, the Government may require them to be remediated before a provisional authorization is issued.
e) The contractor is responsible for mitigating all security risks found during A&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 30 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

13) Authorization of System

The contractor shall provide access to the Federal Government, or their designee acting as their

agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. The Government reserves the right to conduct onsite inspections. The contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this review.

14) Reporting and Continuous Monitoring

Maintenance of the FedRAMP Provisional Authorization will be through continuous monitoring and periodic audit of the operational controls within a contractor's system, environment, and processes to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to the FedRAMP PMO as required by FedRAMP Requirements. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. The deliverables will allow the FedRAMP JAB to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. Contractors will be required to provide updated deliverables and automated data feeds as defined in the FedRAMP Continuous Monitoring Plan.

All deliverables shall be labeled appropriately (such as "Controlled Unclassified Information" (CUI)). External transmission/dissemination of labeled deliverables to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140 (as amended), "Security requirements for Cryptographic Modules."

15) Non-Repudiation

The Cloud Service Provider vendor shall provide a system that is capable of implementing NIST SP 800-53 Control AU-10 approved controls, which provides for origin authentication, data integrity, and signer non-repudiation. This binds the identity of the information producer with the information to and provides the means for authorized individuals to determine the identity of the producer of the information.

16) Identification and Authentication (Organizational Users)

The vendor shall support a secure, multi-factor method of remote authentication and authorization to identified Government Administrators that will allow Government designated personnel the ability to perform management duties on the system.

The vendor shall support multi-factor authentication including user ID and Password, digital certificate, PIV or smart card, PIN, tokens, etc.

17) Identification and Authentication (Non-Organizational Users)

The vendor shall support a secure, dual factor method of remote authentication and authorization to identified Vendor Administrators that will allow vendor-designated personnel the ability to perform management duties on the system.

18) Incident Reporting Timeframes

Cloud Service Providers are required to report all computer security incidents to the United States Computer Emergency Readiness Team (U.S.-CERT) in accordance with U.S.-CERT "Incident Categories and Reporting Timeframes" in, Appendix J, Table J-1 of NIST SP 800-61 (as amended), "Computer Security Incident Handling Guide." Any Category (CAT) 1, CAT 2, or CAT 3 incident, must be reported immediately to their Information Systems Security Officer (ISSO) and the Senior Agency Information Security Officer (SAISO). Any incident that involves compromised Personally Identifiable Information (PII) must be reported to U.S.-CERT within 1 hour of detection regardless of the incident category reporting timeframe.

19) Media Transport

The vendor shall document activities associated with the transport of Federal agency information stored on digital and non-digital media and employ cryptographic mechanisms to protect the confidentiality and integrity of this information during transport outside of controlled areas. Digital media, containing Federal agency information, that is transported outside of controlled areas must be encrypted using an approved encryption mode; non-digital media including but not limited to CD-ROM, floppy disks, etc., must be secured using the same policies and procedures as paper.

Media, containing Federal Agency information that is transported outside of controlled areas must ensure accountability. This can be accomplished through appropriate actions such as logging and a documented chain of custody form.

Federal Agency data that resides on mobile/portable devices (e.g., USB flash drives, external hard 12 drives, and SD cards) must be encrypted using an approved encryption mode. All Federal Agency data residing on laptop computing devices must be protected with approved encryption software.

20) Boundary Protection

The CSP/Reseller shall route all external connections through a Trusted Internet Connection (TIC).

21) Protection of Information At Rest

The CSP shall provide security mechanisms for handling data at rest and in transit in accordance with FIPS 140-2.

22) Security Alerts, Advisories, and Directives

The CSP/Reseller shall provide a list of their personnel, identified by name and role, with system 1 administration, monitoring, and/or security responsibilities that are to receive security alerts, two advisories, and directives. This list shall include ICE SOC.

H.11. PRIVACY EXPECTATIONS

Government contractor employees do not have a right, nor should they have an expectation, of privacy while using Government provided devices at any time, including accessing the Internet and using e-mail and voice communications. To the extent that employees wish that their private activities remain private, they should avoid using the Government provided device for limited personal use. By acceptance of the government provided device, employees imply their consent to disclosing and/or monitoring of device usage, including the contents of any files or information maintained or passed -through that device.

H.12. CONTRACTOR IT SECURITY ACCREDITATION

Within 6 months after contract, the contractor shall submit written proof of IT Security accreditation to DHS for approval by DHS CO. Accreditation will proceed according to the criteria of DHS Sensitive System Policy Publication, 4300A (most current version) or any replacement publication, which the CO will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the CO, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

H.13. SUPPLY CHAIN RISK MANAGEMENT TERMS AND CONDITIONS

The contractors supplying the Government hardware and software shall provide the manufacturer's name, address, state and/or domain of registration, and the Data Universal Numbering System (DUNS) number for all components comprising the hardware and software. If subcontractors or subcomponents are used, the name, address, state, and/or domain of registration and DUNs number of those suppliers must also be provided.

Subcontractors are subject to the same general requirements and standards as prime contractors. Contractors employing subcontractors shall perform due diligence to ensure that these standards are met.

The Government shall be notified when a new contractor/subcontractor/service provider is introduced to the supply chain, or when suppliers of parts or subcomponents are changed. Contractors shall provide, implement, and maintain a Supply Chain Risk Management Plan that addresses internal and external practices and controls employed to minimize the risk posed by counterfeits and vulnerabilities in systems, components, and software.

The Plan shall describe the processes and procedures that will be followed to ensure appropriate supply chain protection of information system resources developed, processed, or used under this contract.

The Supply Chain Risk Management Plan shall address the following elements:

(i) How risks from the supply chain will be identified;
(ii) What processes and security measures will be adopted to manage these risks to the system or system components; and
(iii) How the risks and associated security measures will be updated and monitored.

The Supply Chain Risk Management Plan shall remain current through the life of the contract or period of performance. The Supply Chain Risk Management Plan shall be provided to the Contracting Officer Representative (COR/CO) 30 days post award.

The contractor acknowledges the Government's requirement to assess the Contractors Supply Chain Risk posture. The Contractor understands and agrees that the Government retains the right to cancel or terminate the contract, if the Government determines that continuing the contract presents a risk to national security.

The contractor shall disclose, and the Government will consider, relevant industry standard certifications, recognitions and awards, and acknowledgments.

The contractor shall provide only new equipment unless otherwise expressly approved, in writing, by the CO. Contractors shall provide only Original Equipment Manufacturer (OEM) parts to the Government. In the event that a shipped OEM part fails, all replacement parts must be OEM parts.

The contractor shall be excused from using new OEM (i.e. "grey market, "previously used) components only with formal Government approval. Such components shall be procured from their original source and have them shipped only from manufacturers authorized shipment points.

For software products, the contractor shall provide all OEM software updates to correct defects for the life of the product (i.e., until the “end of life"). Software updates and patches must be made available to the government for all products procured under this contract.

Contractors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is documented at all times from initial shipping point to final destination, and every transfer of the component from one custodian to another is fully documented and accountable) for all shipments to fulfill contract obligations with the Government.

All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lessor of the term of the contract, the period of performance, or one calendar year from the date the activity occurred.

These records must be readily available for inspection by any agent designated by the U.S. Government as having the authority to examine them.

This transit process shall minimize the number of times en route components undergo a change of custody and make use of tamper-proof or tamper-evident packaging for all shipments. The

supplier, at the Government's request, shall be able to provide shipping status at any time during transit.

The contractor is fully liable for all damage, deterioration, or losses incurred during shipping and handling, unless the damage, deterioration, or loss is due to the Government. The contractor shall provide a packing slip which shall accompany each container or package with the information identifying the contract number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact. The contractor shall send a shipping notification to the intended government recipient or contracting officer. This shipping notification shall be sent electronically and will state the contract number, the order number, a description of the hardware/software being ship (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

H.14. REQUIRED PROTECTIONS FOR DHS/ICE SYSTEMS HOSTED IN NON-DHS/ICE DATA CENTERS

1) Security Authorization Terms and Conditions

A Security Authorization of any infrastructure directly in support of DHS/ICE information system shall be performed as a general support system (GSS) prior to DHS/ICE occupancy to characterize the network, identify threats, identify vulnerabilities, analyze existing and planned security controls, determine likelihood of threat, analyze impact, determine risk, recommend controls, perform remediation on identified deficiencies, and document the results. The Security Authorization (SA) shall be performed in accordance with DHS/ICE Security Policy and the controls provided by the hosting provider shall be equal to or stronger than the FIPS 199 security categorization of DHS/ICE information system.

At the beginning of the contract, and upon request thereafter (generally at the deployment of a new system or renewal of a System Authority to Operate), the contractor/Cloud Service Provider (CSP) shall provide the results of an independent assessment and verification of security controls. The independent assessment and verification shall apply the same standards that DHS/ICE applies in the SA process of its information systems. Any deficiencies noted during this assessment shall be provided to the COR for entry into DHS/ICE POA&M Management Process. ICE shall use DHS' 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 shall be corrected within the timeframes dictated by DHS/ICE POA&M Management Process. CSP procedures shall be subject to periodic, unannounced assessments by DHS/ICE officials. The documented physical aspects associated with CSP activities shall also be subject to such assessments. Inspections of CSP physical facilities will be scheduled in advance and coordinated with the provider in accordance with their facility procedures. On a periodic basis, DHS and its Components, including DHS Office of Inspector General, may choose to evaluate any or all of the security controls implemented by the contractor under these clauses. Evaluation could include, but is not limited to vulnerability scanning. The DHS and its Components reserve the right to conduct audits at their discretion. With ten working days' notice, at the request of the Government, the CSP and reseller shall fully

cooperate and facilitate in a Government-sponsored security control assessment at each location wherein DHS/ICE information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of DHS/ICE, including those initiated by the Office of the Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) determined by DHS/ICE in the event of a security incident.

2) Enterprise Security Architecture Terms and Conditions

The CSP shall utilize and adhere to DHS/ICE Enterprise Security Architecture in accordance with applicable laws and DHS/ICE policies to the satisfaction of DHS/ICE COR.

3) Continuous Monitoring Terms and Conditions

The CSP shall participate in the DHS/ICE Continuous Monitoring methodologies and, shall provide a Continuous Monitoring capability over their resources as required by FedRAMP. The DHS Chief Information Security Officer (CISO) issues annual updates to its Continuous Monitoring requirements via the Annual Information Security Performance Plan. At a minimum, the CSP shall adhere to all ITAR and FedRAMP continuous monitoring requirements and ensure that DHS/ICE can implement and integrate the following processes:

a) Asset Management
b) Vulnerability Management
c) Configuration Management
d) Malware Management
e) Log Integration
f) Security Information Event Management (SIEM) Integration
g) Patch Management
h) Providing near-real-time security status information to DHS/ICE SOC Specific Protections Terms and Conditions
    i) Specific protections that shall be provided by the CSP include, but are not limited to the following:

Specific Operations Terms and Conditions

The contractor shall operate a SOC to provide security for the below mentioned services. The CSP shall support regular reviews with DHS/ICE Information Security Office to coordinate and synchronize the security posture of the CSP hosting facility with that of DHS Data Centers. The SOC personnel shall provide 24x7x365 staff to monitor the network and all of its devices. The CSP staff shall also analyze the information generated by the devices for security events, respond to real-time events, correlate security device events, and perform continuous monitoring. It is recommended that the CSP staff shall also maintain a trouble ticket system in which incidents and outages are recorded. In the event of an incident, the CSP facility SOC shall adhere to the incident response plan.

4) Computer Incident Response Services Terms and Conditions

The CSP shall provide Computer Incident Response Team (CIRT) services. The CSP shall adhere to the standard Incident Reporting process as determined by the Component and is defined by a DHS/ICE-specific incident response plan that adheres to DHS/ICE policy and

procedure for reporting incidents. The CSP shall conduct Incident Response Exercises to ensure all personnel are familiar with the plan. The CSP shall notify DHS/ICE SOC of any incident in accordance with the Incident Response Plan and work with DHS/ICE throughout the incident duration.

5) Network Intrusion Detection Systems (NIDS) and Monitoring Terms and Conditions

The contractor shall provide the design, configuration, implementation, and maintenance of the sensors and hardware that are required to support the NIDS solution. The contractor is responsible for creating and maintaining the NIDS rule sets for their facility(s). The NIDS solution should provide real-time alerts. These alerts and other relevant information shall be located in a central repository. The NIDS shall operate 24x7x365. A summary of alerts shall be made available to DHS/ICE upon request. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS/ICE point of contact in accordance with the incident response plan.

6) Physical and Information Security and Monitoring Terms and Conditions

The CSP shall provide a facility using appropriate protective measures to provide for physical security. All facilities will be located within the United States. The CSP shall maintain a process to control physical access to all DHS/ICE IT assets. DHS/ICE IT Assets shall be monitored 24x7x365. A summary of unauthorized access attempts shall be reported to the appropriate DHS/ICE security office upon request.

7) Vulnerability Assessments Terms and Conditions

The CSP and reseller shall provide all information from any managed device to DHS/ICE, as requested, and shall assist, as needed, to perform periodic vulnerability assessments of the network, operating systems, and applications to identify vulnerabilities and propose mitigations. Vulnerability assessments shall be included as part of compliance with the continuous monitoring of the system.

8) Anti-malware (e.g., virus, spam) Terms and Conditions

The CSP shall design, implement, monitor, and manage to provide comprehensive anti-malware service. The CSP shall provide all maintenance for the system providing the anti-malware capabilities to include configuration, definition updates, when changes are required. A summary of alerts shall be reported to DHS/ICE SOC in weekly status report. If an abnormality or anomaly is identified, the CSP shall notify the appropriate DHS/ICE point of contact in accordance with the incident response plan.

9) Log Retention Terms and Conditions

Log files for all infrastructure devices, physical access, and anti-malware should be retained online for 180 days and offline for three years.

H.15. PATCH MANAGEMENT TERMS AND CONDITIONS

The CSP, or software vendor (for certain Software-as-a-Service (SaaS) offerings), shall perform

patch management services to all Platform-as-a-Service (PaaS) and SaaS offerings managed by the CSP, or in cases where the SaaS offering is hosted by an independent third party, the third party will be responsible for providing the patch management services. The CSP shall push patches that are required by vendors and DHS/ICE system owner. This is to ensure that the infrastructure and applications that directly support DHS/ICE information system are current in their release and that all security patches are applied. The CSP and software vendor shall be informed by DHS/ICE which patches are required by DHS/ICE through the Information Security Vulnerability Management bulletins and advisories. Core applications, the ones DHS/ICE utilizes to fulfill their mission, shall be tested by DHS/ICE. However, the CSP and software vendor(s) shall be responsible for deploying patches to their products as directed by DHS/ICE. It is recommended that all other applications (host-based intrusion detection system (HIDS), network intrusion detection system (NIDS), Anti-malware, and Firewall) shall be tested by the CSP prior to deployment in a test environment.

[END OF SECTION H]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION I:
CONTRACT CLAUSES

I.1. FAR CLAUSES AND/OR PROVISIONS INCORPORATED BY REFERENCE

Notice:
System updates may lag policy updates. The System for Award Management (SAM) may continue to require entities to complete representations based on provisions that are not included in agency solicitations. Examples include 52.222-25, Affirmative Action Compliance, and paragraph (d) of 52.212-3, 52.223-22, Public Disclosure of Greenhouse Gas Emissions and Reduction Goals—Representation, and Offeror Representations and Certifications—Commercial Products and Commercial Services, including paragraph (t). Additional examples include 52.212-5, Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Products and Commercial Services, and 52.213-4, Terms and Conditions—Simplified Acquisitions (Other Than Commercial Products and Commercial Services).

Contracting officers will **not** consider the following representations when making award decisions or enforcing requirements:

- Paragraph (d) and (t) of 52.212-3, Offeror Representations and Certifications—Commercial Products and Commercial Services

- Paragraphs (b)(33), (b)(34), (e)(1)(ix), and (e)(1)(x) of 52.212-5, Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Products and Commercial Services. Additionally, per this deviation, in paragraph (b)(46), E.O. 14057 does not apply;

- Paragraphs (e)(1)(ii)(I) and (e)(1)(ii)(J) of Alternate II of 52.212-5, Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Products and Commercial Services

- Paragraphs (a)(1)(vii) and (a)(1)(viii) of 52.213-4, Terms and Conditions—Simplified Acquisitions (Other Than Commercial Products and Commercial Services). Additionally, per this deviation, in paragraph (b)(1)(xvii), E.O. 14057 does not apply.

  Entities are not required to update their entity registration to remove these representations in SAM.

The following clauses and/or provisions are incorporated by reference.

Number	Title	Date
52.202-1	Definitions	Jun 2020
52.203-12	Limitation on Payments to Influence Certain Federal Transactions	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
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards (DEVIATION 25-19)	Aug 2025
52.204-13	System for Award Management Maintenance (DEVIATION 25-19)	Aug 2025
52.204-14	Service Contract Reporting Requirements (DEVIATION 25-19)	Aug 2025
52.204-19	Incorporation by Reference of Representations and Certifications	Dec 2014
52.204-22	Alternative Line Item Proposal	Jan 2017
52.208-9	Contractor Use of Mandatory Sources of Supply or Services (DEVIATION 25-20)	Aug 2025
52.209-6	Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended, Proposed for Debarment, or Voluntarily Excluded (DEVIATION 25-27)	Nov 2025
52.209-9	Updates of Publicly Available Information Regarding Responsibility Matters (DEVIATION 25-27)	Nov 2025
52.209-10	Prohibition on Contracting with Inverted Domestic Corporations (DEVIATION 25-27)	Nov 2025
52.212-4	Contract Terms and Conditions—Commercial Products and Commercial Services - (DEVIATION 25-21)	Aug 2025
52.219-8	Utilization of Small Business Concerns (DEVIATION 26-03)	Oct 2025
52.219-14	Limitations on Subcontracting (DEVIATION 26-03)	Oct 2025
52.219-28	Postaward Small Business Program Rerepresentation (DEVIATION 26-03)	Oct 2025
52.222-35	Equal Opportunity For Veterans (DEVIATION 26-10)	Oct 2025
52.222-36	Equal Opportunity for Workers with Disabilities (DEVIATION 26-10)	Oct 2025
52.222-37	Employment Reports On Veterans (DEVIATION 26-10)	Oct 2025
52.222-40	Notification of Employee Rights Under the National Labor Relations Act.	Dec 2010
52.222-41	Service Contract Labor Standards.	Aug 2018
52.222-42	Statement of Equivalent Rates for Federal Hires.	May 2014
52.222-43	Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (Multiple Year and Option Contracts).	Aug 2018
52.222-50	Combating Trafficking in Persons	Nov 2021
52.222-54	Employment Eligibility Verification (DEVIATION 26-10)	Oct 2025
52.222-55	Minimum Wages for Contractor Workers Under Executive Order 14026. (DEVIATION)	Jan 2022
52.222-62	Paid Sick Leave Under Executive Order 13706.	Jan 2022
52.223-3	Hazardous Material Identification and Material Safety Data – Alt I (DEVIATION 26-12)	Oct 2025 Alt I Oct 2025

52.223-5	Pollution Prevention and Right-to-Know Information	May 2024
52.223-23	Sustainable Products and Services (DEVIATION 26-12)	Oct 2025
52.224-1	Privacy Act Notification	Apr 1984
52.224-2	Privacy Act	Apr 1984
52.224-3	Privacy Training – Alternate I*	Jan 2017 Alt I Jan 2017
52.226-7	Drug-Free Workplace	May 2024
52.226-8	Encouraging Contractor Policies to Ban Text Messaging While Driving	May 2024
52.227-14	Rights in Data—General	May 2014
52.227-17	Rights in Data-Special Works	Dec 2007
52.229-3	Federal, State, and Local Taxes	Feb 2013
52.229-12	Tax on Certain Foreign Procurements	Feb 2021
52.232-1	Payments	Apr 1984
52.232-11	Extras	Apr 1984
52.232-17	Interest	May 2014
52.232-33	Payment by Electronic Funds Transfer-System for Award Management	Oct 2018
52.232-39	Unenforceability of Unauthorized Obligations	Jun 2013
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	Mar 2023
52.233-3	Protest after Award (DEVIATION 25-25)	Aug 2025
52.233-4	Applicable Law for Breach of Contract Claim (DEVIATION 25-25)	Aug 2025
52.237-2	Protection of Government Buildings, Equipment, and Vegetation	Apr 1984
52.237-3	Continuity of Services	Jan 1991
52.242-13	Bankruptcy	Jul 1995

I.2. FAR CLAUSES AND/OR PROVISIONS INCORPORATED BY FULL TEXT

The following clauses and/or provisions are incorporated by full text.

52.217-9 Option to Extend the Term of the Contract (Mar 2020)

(a) The Government may extend the term of this contract by written notice to the Contractor within 15 days before expiration of the contract; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 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 48 months.

(End of clause)

52.224-3 Privacy Training – Alternate I (DEVIATION)

(a) Definition. As used in this clause, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) Circular A–130, Managing Federal Information as a Strategic Resource).

(b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who—

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or

(3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing Privacy at DHS: Protecting Personal Information accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.

(d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.

(e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will—

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or

(3) Design, develop, maintain, or operate a system of records.

(End of clause)

52.240-91 Security Prohibitions and Exclusions (Aug 2025) (DEVIATION 25-23)

(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 arrangements 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 clause)

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 address: https://www.acquisition.gov.

(End of clause)

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 FAR clause or Homeland Security Acquisition Regulation (48 CFR Chapter 30) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of Clause)

I.3. HSAR CLAUSES AND/OR PROVISIONS INCORPORATED BY REFERENCE

3052.212-70 Contract Terms and Conditions Applicable to DHS Acquisition of Commercial Items (July 2023)

The Contractor agrees to comply with any provision or clause that is incorporated herein by reference to implement agency policy applicable to acquisition of commercial items or components. The provision or clause in effect based on the applicable regulation cited on the date the solicitation is issued applies unless otherwise stated herein. The following provisions and clauses are incorporated by reference:

(a) *Provisions.*

(b) *Clauses.*

3052.203-70, Instructions for Contractor Disclosure of Violations

3052.204-71 Contractor Employee Access—Alternate II

3052.204-72 Safeguarding of Controlled Unclassified Information – Alternate I

3052.204-73 Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents

3052.205-70 Advertisement, Publicizing Awards, and Releases

3052.215-70 Key Personnel or Facilities

3052.228-70 Insurance

3052.242-72 Contracting Officer's Representative

(End of clause)

HSAR 3052.219-71 DHS Mentor-Protégé Program (DEVIATION) (Apr 2024)

(a) Large businesses are encouraged to participate in the DHS Mentor-Protégé program for the purpose of providing developmental assistance to eligible protégé entities to enhance their capabilities and increase their participation in DHS contracts.

(b) The program consists of:

(1) Mentor firms, which are large prime contractors capable of providing developmental assistance;

(2) Protégé firms, are small businesses, veteran-owned small businesses, service-disabled veteran-owned small businesses, HUBZone small businesses, small-disadvantaged businesses, and women-owned small business concerns, Historically Black Colleges and Universities, and Minority Serving Institutions; and

(3) Mentor-Protégé agreements, approved by the DHS Office of Small and Disadvantaged Business Utilization (OSDBU).

(c) Mentor participation in the program means providing business developmental assistance to aid protégés in developing the requisite expertise to effectively compete for and successfully perform DHS contracts and subcontracts.

(d) Large business prime contractors serving as mentors in the DHS Mentor-Protégé program are eligible for a post-award incentive for subcontracting plan credit. The mentor may receive small

business subcontracting credit for costs it incurs to provide assistance to a protégé. The mentor may use this additional credit towards attaining its subcontracting plan participation goal under the same or another DHS contract. The amount of credit given to a mentor firm for these protégé developmental assistance costs shall be calculated on a dollar-for-dollar basis and reported in the Summary Subcontract Report via the Electronic Subcontracting Reporting System (eSRS) at www.esrs.gov. For example, a mentor/large business prime contractor would report a $10,000 subcontract to the protégé subcontractor and $5,000 of developmental assistance to the protégé as $15,000. The Mentor and Protégé will submit a signed joint statement agreeing on the dollar value of the developmental assistance and the Summary Subcontract Report.

(e) Contractors interested in participating in the program are encouraged to contact the DHS OSDBU for more information.

(End of clause)

I.4. HSAR CLAUSES AND/OR PROVISIONS INCORPORATED BY FULL TEXT

3052.204-72 Safeguarding of Controlled Unclassified Information (July 2023)

(a) Definitions. As used in this clause—

Adequate Security means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

Controlled Unclassified Information (CUI) is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, "Chemical Facility Anti-Terrorism Standards," and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual "Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information" dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116–283), PCII's implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, "Protection of Sensitive Security Information," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or designee), including Department of Homeland Security MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2810.1, "SSI Program";

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

(i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is

responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, the DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits);
(B) Date of birth (month, day, and year);
(C) Citizenship or immigration status;
(D) Ethnic or religious affiliation;
(E) Sexual orientation;
(F) Criminal history;
(G) Medical information; and
(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

Federal information means information created, collected, processed, maintained, disseminated,

disclosed, or disposed of by or for the Federal Government, in any medium or form.
Federal information system means an information system used or operated by an agency or by a Contractor of an agency or by another organization on behalf of an agency.

Handling means any use of controlled unclassified information, including but not limited to marking, safeguarding, transporting, disseminating, re-using, storing, capturing, and disposing of the information.

Incident means an occurrence that—

(1) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

(2) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Information Resources means information and related resources, such as personnel, equipment, funds, and information technology.

Information Security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(1) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(2) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(3) Availability, which means ensuring timely and reliable access to and use of information.

Information System means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

(b) Handling of Controlled Unclassified Information.

(1) Contractors and subcontractors must provide adequate security to protect CUI from unauthorized access and disclosure. Adequate security includes compliance with DHS policies and procedures in effect at the time of contract award. These policies and procedures are accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors.

(2) The Contractor shall not use or redistribute any CUI handled, collected, processed, stored, or transmitted by the Contractor except as specified in the contract.

(3) The Contractor shall not maintain SPII in its invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions. It is acceptable to maintain in these systems the names, titles, and contact information for the Contracting Officer’s Representative

(COR) or other government personnel associated with the administration of the contract, as needed.

(4) Any government data provided, developed, or obtained under the contract, or otherwise under the control of the Contractor, shall not become part of the bankruptcy estate in the event a Contractor and/or subcontractor enters bankruptcy proceedings.

(c) Incident Reporting Requirements.

(1) Contractors and subcontractors shall report all known or suspected incidents to the Component Security Operations Center (SOC) in accordance with Attachment F, Incident Response, to DHS Policy Directive 4300A Information Technology System Security Program, Sensitive Systems. If the Component SOC is not available, the Contractor shall report to the DHS Enterprise SOC. Contact information for the DHS Enterprise SOC is accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors. Subcontractors are required to notify the prime Contractor that it has reported a known or suspected incident to the Department. Lower tier subcontractors are required to likewise notify their higher tier subcontractor, until the prime contractor is reached. The Contractor shall also notify the Contracting Officer and COR using the contact information identified in the contract. If the report is made by phone, or the email address for the Contracting Officer or COR is not immediately available, the Contractor shall contact the Contracting Officer and COR immediately after reporting to the Component or DHS Enterprise SOC.

(2) All known or suspected incidents involving PII or SPII shall be reported within 1 hour of discovery. All other incidents shall be reported within 8 hours of discovery.

(3) CUI transmitted via email shall be protected by encryption or transmitted within secure communications systems. CUI shall be transmitted using a FIPS 140-2/140-3 Security Requirements for Cryptographic Modules validated cryptographic module identified on https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules. When this is impractical or unavailable, for Federal information systems only, CUI may be transmitted over regular email channels. When using regular email channels, Contractors and subcontractors shall not include any CUI in the subject or body of any email. The CUI shall be included as a password-protected attachment with the password provided under separate cover, including as a separate email. Recipients of CUI information will comply with any email restrictions imposed by the originator.

(4) An incident shall not, by itself, be interpreted as evidence that the Contractor or Subcontractor has failed to provide adequate information security safeguards for CUI or has otherwise failed to meet the requirements of the contract.

(5) If an incident involves PII or SPII, in addition to the incident reporting guidelines in Attachment F, Incident Response, to DHS Policy Directive 4300A Information Technology System Security Program, Sensitive Systems, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Unique Entity Identifier (UEI);
(ii) Contract numbers affected unless all contracts by the company are affected;

(iii) Facility CAGE code if the location of the event is different than the prime Contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, and email);
(v) Contracting Officer POC (address, telephone, and email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms, or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where CUI resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the government PII or SPII contained within the system; and
(xiii) Any additional information relevant to the incident.

(d) Incident Response Requirements.

(1) All determinations by the Department related to incidents, including response activities, will be made in writing by the Contracting Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections;
(ii) Investigations;
(iii) Forensic reviews;
(iv) Data analyses and processing; and
(v) Revocation of the Authority to Operate (ATO), if applicable.

(4) The Contractor shall immediately preserve and protect images of known affected information systems and all available monitoring/packet capture data. The monitoring/packet capture data shall be retained for at least 180 days from submission of the incident report to allow DHS to request the media or decline interest.

(5) The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(e) Certificate of Sanitization of Government and Government-Activity-Related Files and Information. Upon the conclusion of the contract by expiration, termination, cancellation, or as otherwise indicated in the contract, the Contractor shall return all CUI to DHS and/or destroy it physically and/or logically as identified in the contract unless the contract states that return and/or destruction of CUI is not required. Destruction shall conform to the guidelines for media sanitization contained in NIST SP 800–88, Guidelines for Media Sanitization. The Contractor shall certify and

confirm the sanitization of all government and government-activity related files and information. The Contractor shall submit the certification to the COR and Contracting Officer following the template provided in NIST SP 800–88, Guidelines for Media Sanitization, Appendix G.

(f) Other Reporting Requirements. Incident reporting required by this clause in no way rescinds the Contractor's responsibility for other incident reporting pertaining to its unclassified information systems under other clauses that may apply to its contract(s), or as a result of other applicable statutory or regulatory requirements, or other U.S. Government requirements.

(g) Subcontracts. The Contractor shall insert this clause in all subcontracts and require subcontractors to include this clause in all lower tier subcontracts when subcontractor employees will have access to CUI; CUI will be collected or maintained on behalf of the agency by a subcontractor; or a subcontractor information system(s) will be used to process, store, or transmit CUI.
(End of clause)

ALTERNATE I (JULY 2023)

When Federal information systems, which include Contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI, add the following paragraphs:

(h) Authority to Operate. The Contractor shall not collect, process, store, or transmit CUI within a Federal information system until an ATO has been granted by the Component or Headquarters CIO, or designee. Once the ATO has been granted by the Government, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. Unless otherwise specified in the ATO letter, the ATO is valid for 3 years. An ATO is granted at the sole discretion of the Government and can be revoked at any time. Contractor receipt of an ATO does not create any contractual right of access or entitlement. The Government's grant of an ATO does not alleviate the Contractor's responsibility to ensure the information system controls are implemented and operating effectively.

(1) Complete the Security Authorization process. The Security Authorization (SA) process shall proceed according to DHS Policy Directive 4300A Information Technology System Security Program, Sensitive Systems (Version 13.3, February 13, 2023), or any successor publication; and the Security Authorization Process Guide, including templates. These policies and templates are accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors.

(i) Security Authorization Package. The SA package shall be developed using the government-provided Security Requirements Traceability Matrix and SA templates. The SA package consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). The Contractor shall submit a signed copy of the SA package, validated by an independent third party, to the COR for review and approval by the Component or Headquarters CIO, or designee, at least 30 days prior to the date of operation of the information system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of modified documents.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the information system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in NIST SP 800–53, Security and Privacy Controls for Information Systems and Organizations, or successor publication, accessible at https://csrc.nist.gov/publications/sp. The Contractor shall address all deficiencies before submitting the SA package to the COR for review.

(2) Renewal of ATO. Unless otherwise specified in the ATO letter, the Contractor shall renew the ATO every 3 years. The Contractor is required to update its SA package as part of the ATO renewal process for review and verification of security controls. Review and verification of security controls is independent of the system production date and may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place. The updated SA package shall be submitted for review and approval by the Component or Headquarters CIO, or designee, at least 90 days before the ATO expiration date. The Contractor shall update its SA package by one of the following methods:

(i) Updating the SA package in the DHS Information Assurance Compliance System; or

(ii) Submitting the updated SA package directly to the COR.

(3) Security Review. The Government may elect to conduct periodic reviews to ensure that the security requirements contained in the contract are being implemented and enforced. The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in security review activities. The Contractor shall afford DHS, the Office of the Inspector General, other government organizations, and Contractors working in support of the Government access to the Contractor's facilities, installations, operations, documentation, databases, networks, systems, and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Component or Headquarters CIO, or designee, to coordinate and participate in review and inspection activity by government organizations external to DHS. Access shall be provided, to the extent necessary as determined by the Government (including providing all requested images), for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) Federal Reporting and Continuous Monitoring Requirements. Contractors operating information systems on behalf of the Government shall comply with Federal reporting and information system continuous monitoring requirements. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2015 DHS Information Security Performance Plan, or successor publication, accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors. The plan is updated on an annual basis. Annual, quarterly, and monthly data collection will be coordinated by the Government. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for information systems. The Contractor shall provide the COR with requested information within 3 business days of receipt of the request. Unless otherwise specified in the contract, monthly continuous monitoring data shall be stored at the

Contractor's location for a period not less than 1 year from the date the data are created. The Government may elect to perform information system continuous monitoring and IT security scanning of information systems from government tools and infrastructure.

(End of clause)

3052.204-73 Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents (July 2023)

(a) *Definitions.* Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, the DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(1) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(2) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(i) Truncated SSN (such as last 4 digits);
(ii) Date of birth (month, day, and year);
(iii) Citizenship or immigration status;
(iv) Ethnic or religious affiliation;
(v) Sexual orientation;
(vi) Criminal history;
(vii) Medical information; and
(viii) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(3) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone

number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

(b) *PII and SPII Notification Requirements.*

(1) No later than 5 business days after being directed by the Contracting Officer, or as otherwise required by applicable law, the Contractor shall notify any individual whose PII or SPII was either under the control of the Contractor or resided in an information system under control of the Contractor at the time the incident occurred. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by, the Contracting Officer. The Contractor shall not proceed with notification unless directed in writing by the Contracting Officer.

(2) All determinations by the Department related to notifications to affected individuals and/or Federal agencies and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer.

(3) Subject to government analysis of the incident and direction to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first-class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII or SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, mitigate the incident, and protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(c) *Credit Monitoring Requirements.* The Contracting Officer may direct the Contractor to:

(1) Provide notification to affected individuals as described in paragraph (b).

(2) Provide credit monitoring services to individuals whose PII or SPII was under the control of the Contractor or resided in the information system at the time of the incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts.

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized Frequently Asked Questions, approved in writing by the Contracting Officer in coordination with the Component or Headquarters Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(End of clause)

3052.209-70 Prohibition on Contracts with Corporate Expatriates (Jun 2006)

(a) Prohibitions.
Section 835 of the Homeland Security Act, 6 U.S.C. 395, prohibits the Department of Homeland Security from entering into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation as defined in this clause, or with any subsidiary of such an entity. The Secretary shall waive the prohibition with respect to any specific contract if the Secretary determines that the waiver is required in the interest of national security.
(b) Definitions. As used in this clause:
Expanded Affiliated Group means an affiliated group as defined in section 1504(a) of the Internal Revenue Code of 1986 (without regard to section 1504(b) of such Code), except that section 1504 of such Code shall be applied by substituting `more than 50 percent' for `at least 80 percent' each place it appears.
Foreign Incorporated Entity means any entity which is, or but for subsection (b) of section 835 of the Homeland Security Act, 6 U.S.C. 395, would be, treated as a foreign corporation for purposes of the Internal Revenue Code of 1986.
Inverted Domestic Corporation means a foreign incorporated entity shall be treated as an inverted domestic corporation if, pursuant to a plan (or a series of related transactions)—
(1) The entity completes the direct or indirect acquisition of substantially all of the properties held directly or indirectly by a domestic corporation or substantially all of the properties constituting a trade or business of a domestic partnership;
(2) After the acquisition at least 80 percent of the stock (by vote or value) of the entity is held—
(i) In the case of an acquisition with respect to a domestic corporation, by former shareholders of the domestic corporation by reason of holding stock in the domestic corporation; or
(ii) In the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and
(3) The expanded affiliated group which after the acquisition includes the entity does not have

substantial business activities in the foreign country in which or under the law of which the entity is created or organized when compared to the total business activities of such expanded affiliated group. Person, domestic, and foreign have the meanings given such terms by paragraphs (1), (4), and (5) of section 7701(a) of the Internal Revenue Code of 1986, respectively.

(c) Special rules. The following definitions and special rules shall apply when determining whether a foreign incorporated entity should be treated as an inverted domestic corporation.

(1) Certain stock disregarded. For the purpose of treating a foreign incorporated entity as an inverted domestic corporation these shall not be taken into account in determining ownership:

(i) Stock held by members of the expanded affiliated group which includes the foreign incorporated entity; or

(ii) Stock of such entity which is sold in a public offering related to an acquisition described in section 835(b)(1) of the Homeland Security Act, 6 U.S.C. 395(b)(1).

(2) Plan deemed in certain cases. If a foreign incorporated entity acquires directly or indirectly substantially all of the properties of a domestic corporation or partnership during the 4-year period beginning on the date which is 2 years before the ownership requirements of subsection (b)(2) are met, such actions shall be treated as pursuant to a plan.

(3) Certain transfers disregarded. The transfer of properties or liabilities (including by contribution or distribution) shall be disregarded if such transfers are part of a plan a principal purpose of which is to avoid the purposes of this section.

(d) Special rule for related partnerships. For purposes of applying section 835(b) of the Homeland Security Act, 6 U.S.C. 395(b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the meaning of section 482 of the Internal Revenue Code of 1986) shall be treated as a partnership.

(e) Treatment of Certain Rights.

(1) Certain rights shall be treated as stocks to the extent necessary to reflect the present value of all equitable interests incident to the transaction, as follows:

(i) warrants;

(ii) options;

(iii) contracts to acquire stock;

(iv) convertible debt instruments; and

(v) other similar interests.

(2) Rights labeled as stocks shall not be treated as stocks whenever it is deemed appropriate to do so to reflect the present value of the transaction or to disregard transactions whose recognition would defeat the purpose of Section 835.

(f) Disclosure. The Offeror under this solicitation represents that [Check one]:

it is not a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003;

it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it has submitted a request for waiver pursuant to 3009.108-7004, which has not been denied; or

it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it plans to submit a request for waiver pursuant to 3009.108-7004.

(g) A copy of the approved waiver, if a waiver has already been granted, or the waiver request, if a waiver has been applied for, shall be attached to the bid or proposal.

(End of Clause)

3052.215-70 Key personnel or facilities (Dec 2003)

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.
(b) Before removing or replacing any of the specified individuals or facilities, the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel or facilities until the Contracting Officer approves the change.

The Key Personnel or Facilities under this Contract:

a) Program Manager
b) Deputy Program Manager
c) Operations Manager
d) Training Manager
e) Fleet Manager

(End of clause)

52.240-90 Security Prohibitions and Exclusions Representations and Certifications. (DEVIATION 20-05) (NOV 2025)

(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

(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 Attachment 1 FAR Class Deviation
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 $10,000 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

(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 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;
https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx

(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) In the event the Contractor identifies covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report, in writing, via email, to the Contracting Officer, Contracting Officer's Representative, and the Enterprise Security Operations Center (SOC) at NDAA_Incidents@hq.dhs.gov, with required information in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Enterprise SOC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided 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)

52.240-91 Security Prohibitions and Exclusions. (DEVIATION 20-05) (NOV 2025)

(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 arrangements 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—
Attachment 1 FAR Class Deviation 2020-05, Revision 4
FAR Deviation 20-05, Rev 4 Page 10 of 17
(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)).
Attachment 1 FAR Class Deviation 2020-05, Revision 4
FAR Deviation 20-05, Rev 4 Page 11 of 17

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
Attachment 1 FAR Class Deviation 2020-05, Revision 4
FAR Deviation 20-05, Rev 4 Page 12 of 17

(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 $10,000) 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) In the event the Contractor identifies covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report, in writing, via email, to the Contracting Officer, Contracting Officer's Representative, and the Enterprise Security Operations Center (SOC) at NDAA_Incidents@hq.dhs.gov, with required information in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Enterprise SOC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided 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 clause)

Alternate I (DATE XXXX). As prescribed in 40.205(b), substitute the following paragraph (e)(1) for paragraph (e)(1) of the basic clause:

(e) *Governmentwide exclusion and removal orders*.

(1) Contractors are prohibited from providing or using 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 any applicable FASCSA orders identified by the checkbox(es) in this paragraph (e)(1). [*Contracting Officer must select either "yes" or "no" for each of the following types of FASCSA orders*:]

Yes □ No □ DHS FASCSA Order
Yes □ No □ DoD FASCSA Order
Yes □ No □ DNI FASCSA Order

SPECIAL CLAUSE INFORMATION TECHNOLOGY SECURITY AWARENESS TRAINING (JULY 2023)

(a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) Security Training Requirements.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information

under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually, and the COR will provide notification when a review is required.

[END OF SECTION I]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION J:
LIST OF ATTACHMENTS

J.1. LIST OF ATTACHMENTS

Attachment 01- Performance Work Statement
Attachment 02- Pricing Template
Attachment 03- Consolidated Wage Determinations
Attachment 04- Solicitation Question Template

.

[END OF SECTION J]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

PART IV – REPRESENTATIONS AND INSTRUCTIONS

SECTION K:
REPRESENTATIONS, CERTIFICATIONS, AND OTHER STATEMENTS OF OFFERORS OR RESPONDENTS

K1. PROVISIONS INCORPORATED BY REFERENCE

Number	Title	Date
52.203-11	Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions	Sep 2007
52.203-18	Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements—Representation	Jan 2017
52.204-5	Women-Owned Business (Other Than Small Business)	Oct 2014
52.204-17	Ownership or Control of Offeror	Aug 2020
52.225-25	Prohibition on Contracting with Entities Engaging in Certain Activities or Transactions Relating to Iran—Representation and Certifications	Jun 2020

K2. PROVISIONS INCORPORATED IN FULL TEXT

52.203-2 Certificate of Independent Price Determination (Apr 1985)

(a) The offeror certifies that-

(1) The prices in this offer have been arrived at independently, without, for the purpose of restricting competition, any consultation, communication, or agreement with any other offeror or competitor relating to-

(i) Those prices;

(ii) The intention to submit an offer; or

(iii) The methods or factors used to calculate the prices offered.

(2) The prices in this offer have not been and will not be knowingly disclosed by the offeror, directly or indirectly, to any other offeror or competitor before bid opening (in the case of a sealed bid solicitation) or contract award (in the case of a negotiated solicitation) unless otherwise required by law; and

(3) No attempt has been made or will be made by the offeror to induce any other concern to submit or not to submit an offer for the purpose of restricting competition.

(b) Each signature on the offer is considered to be a certification by the signatory that the

signatory-

(1) Is the person in the offeror's organization responsible for determining the prices being offered in this bid or proposal, and that the signatory has not participated and will not participate in any action contrary to paragraphs (a)(1) through (a)(3) of this provision; or

(2) (i) Has been authorized, in writing, to act as agent for the following principals in certifying that those principals have not participated, and will not participate in any action contrary to paragraphs (a)(1) through (a)(3) of this provision _____ [insert full name of person(s) in the offeror's organization responsible for determining the prices offered in this bid or proposal, and the title of his or her position in the offeror's organization];

(ii) As an authorized agent, does certify that the principals named in subdivision (b)(2)(i) of this provision have not participated, and will not participate, in any action contrary to paragraphs (a)(1) through (a)(3) of this provision; and

(iii) As an agent, has not personally participated, and will not participate, in any action contrary to paragraphs (a)(1) through (a)(3) of this provision.

(c) If the offeror deletes or modifies paragraph (a)(2) of this provision, the offeror must furnish with its offer a signed statement setting forth in detail the circumstances of the dis-closure.

52.204-20 Predecessor of Offeror (Aug 2020)

(a) Definitions. As used in this provision–

Commercial and Government Entity (CAGE) code means–

(1) An identifier assigned to entities located in the United States or its outlying areas by the Defense Logistics Agency (DLA) Commercial and Government Entity (CAGE) Branch to identify a commercial or government entity by unique location; or

(2) An identifier assigned by a member of the North Atlantic Treaty Organization (NATO) or by the NATO Support and Procurement Agency (NSPA) to entities located outside the United States and its outlying areas that the DLA Commercial and Government Entity (CAGE) Branch records and maintains in the CAGE master file. This type of code is known as a NATO CAGE (NCAGE) code.

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

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.

(b) 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.

(c) If the Offeror has indicated "is" in paragraph (b) 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).

52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Nov 2021)

The Offeror shall not complete the representation at paragraph (d)(1) of this provision if the Offeror has represented that it "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" in paragraph (c)(1) in the provision at 52.204-26, Covered Telecommunications Equipment or Services—Representation, or in paragraph (v)(2)(i) of the provision at 52.212-3, Offeror Representations and Certifications-Commercial Products or Commercial Services. The Offeror shall not complete the representation in paragraph (d)(2) of this provision if the Offeror has represented that it "does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services" in paragraph (c)(2) of the provision at 52.204-26, or in paragraph (v)(2)(ii) of the provision at 52.212-3.

(a) Definitions. As used in this provision—

Backhaul, covered telecommunications equipment or services, critical technology, interconnection arrangements, reasonable inquiry, roaming, and substantial or essential component have the meanings provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) Prohibition. (1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service 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. Nothing in the prohibition shall be construed to—
(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover 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) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract or extending or renewing a contract with an entity that uses any equipment, system, or service 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. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover 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) Procedures. 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".

(d) Representation. The Offeror represents that—

(1) It ☐ will, ☐ 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. The Offeror shall provide the additional disclosure information required at paragraph (e)(1) of this section if the Offeror responds "will" in paragraph (d)(1) of this section; and

(2) After conducting a reasonable inquiry, for purposes of this representation, the Offeror represents that—

It ☐ does, ☐ does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services. The Offeror shall provide the additional disclosure information required at paragraph (e)(2) of this section if the Offeror responds "does" in paragraph (d)(2) of this section.

(e) Disclosures. (1) Disclosure for the representation in paragraph (d)(1) of this provision. If the Offeror has responded "will" in the representation in paragraph (d)(1) of this provision, the Offeror shall provide the following information as part of the offer:
(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the original equipment manufacturer (OEM) or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(2) Disclosure for the representation in paragraph (d)(2) of this provision. If the Offeror has responded "does" in the representation in paragraph (d)(2) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model

number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the PSC of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

52.204-26 Covered Telecommunications Equipment or Services-Representation (Oct 2020)

(a) Definitions. As used in this provision, "covered telecommunications equipment or services" and "reasonable inquiry" have the meaning provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) Procedures. 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".

(c) (1) Representation. The Offeror represents that 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.
(2) After conducting a reasonable inquiry for purposes of this representation, the offeror represents that it ☐ does, ☐ does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services.

52.209-2 Prohibition on Contracting with Inverted Domestic Corporations-Representation (Nov 2015)

(a) Definitions. "Inverted domestic corporation" and "subsidiary" have the meaning given in the clause of this contract entitled Prohibition on Contracting with Inverted Domestic Corporations (52.209-10).

(b) 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.

(c) Representation. The Offeror represents that-

(1) It ☐ is, ☐ is not an inverted domestic corporation; and

(2) It ☐ is, ☐ is not a subsidiary of an inverted domestic corporation.

52.209-5 Certification Regarding Responsibility Matters (Aug 2020)

(a) (1) The Offeror certifies, to the best of its knowledge and belief, that—
(i) The Offeror and/or any of its Principals–

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

(B) 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 public (Federal, State, or local) 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 (if offeror checks "have", the offeror shall also see 52.209-7, if included in this solicitation);

(C) Are ☐ are not ☐ presently indicted for, or otherwise criminally or civilly charged by a governmental entity with, commission of any of the offenses enumerated in paragraph (a)(1)(i)(B) of this provision;

(D) 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.

(1) Federal taxes are considered delinquent if both of the following criteria apply:

(i) 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.

(ii) 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.

(2) Examples.

(i) The taxpayer has received a statutory notice of deficiency, under I.R.C. § 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.

(ii) 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. § 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.

(iii) The taxpayer has entered into an installment agreement pursuant to I.R.C. § 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.

(iv) 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).

(ii) The Offeror has ☐ has not ☐, within a three-year period preceding this offer, had one or more contracts terminated for default by any Federal agency.

(2) "Principal," for the purposes of this certification, 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).

This Certification Concerns a Matter Within the Jurisdiction of an Agency of the United States and the Making of a False, Fictitious, or Fraudulent Certification May Render the Maker Subject to Prosecution Under Section 1001, Title 18, United States Code.

(b) The Offeror shall provide immediate written notice to the Contracting Officer if, at any time prior to contract award, the Offeror learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

(c) A certification that any of the items in paragraph (a) of this provision exists will not necessarily result in withholding of an award under this solicitation. However, the certification will be considered in connection with a determination of the Offeror’s responsibility. Failure of the Offeror to furnish a certification or provide such additional information as requested by the Contracting Officer may render the Offeror non-responsible.

(d) Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render, in good faith, the certification required by paragraph (a) of this provision. The knowledge and information of an Offeror is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

(e) The certification in paragraph (a) of this provision is a material representation of fact upon which reliance was placed when making award. If it is later determined that the Offeror knowingly rendered an erroneous certification, in addition to other remedies available to the Government, the Contracting Officer may terminate the contract resulting from this solicitation for default.

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).

52.209-11 Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law (Feb 2016)

(a) 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–

(1) 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

(2) 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.

(b) The Offeror represents that–

(1) 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

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

52.212-3 Offeror Representations and Certifications—Commercial Products and Commercial Services (May 2024)

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 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 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"—
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 at13 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 CFR124.104(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 least51 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 __.
[*Offeror to identify the applicable paragraphs at (c) through (v) of this provision that the offeror has completed for the purposes of this solicitation only, if any.*
These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer.
Any changes provided by the offeror are applicable to this solicitation only, and do not result in an update to the representations and certifications posted electronically on SAM.]
(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.* 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 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 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) Representations required to implement provisions of Executive Order11246-

(1) Previous contracts and compliance. The offeror represents that-
(i) It □ has, □ has not participated in a previous contract or subcontract subject to the Equal Opportunity clause of this solicitation; and
(ii) It □ has, □ has not filed all required compliance reports.
(2) *Affirmative Action Compliance*. The offeror represents that-
(i) It □ has developed and has on file, □ has not developed and does not have on file, at each establishment, affirmative action programs required by rules and regulations of the Secretary of Labor (41 CFR parts 60-1 and 60-2), or
(ii) It □ has not previously had contracts subject to the written affirmative action programs requirement of the rules and regulations of the Secretary of Labor.
(e) *Certification Regarding Payments to Influence Federal Transactions (31 http://uscode.house.gov/ U.S.C. 1352)*. (Applies only if the contract is expected to exceed $150,000.) 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 (**
_____	_____	_____
_____	_____	_____
_____	_____	_____

[*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/n**
_____	_____	_____

Line Item No.	Country of Origin	Exceeds 55% domestic content (yes/n
_____	_____	_____
_____	_____	_____

[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.
_____
_____
_____

[*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. §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. §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. §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). [The Contracting Officer must list in paragraph (i)(1) any end products being acquired under this solicitation that are included in the List of Products Requiring Contractor Certification as to Forced or Indentured Child Labor, unless*

excluded at 22.1503(b).]
(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 the 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 CFR1.6049-4;
☐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 e-mail 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 (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) *Public Disclosure of Greenhouse Gas Emissions and Reduction Goals*. Applies in all solicitations that require offerors to register in SAM (12.301(d)(1)).
(1) This representation shall be completed if the Offeror received $7.5 million or more in contract awards in the prior Federal fiscal year. The representation is optional if the Offeror received less than $7.5 million in Federal contract awards in the prior Federal fiscal year.
(2) Representation. [Offeror to check applicable block(s) in paragraph (t)(2)(i) and (ii)].

(i) The Offeror (itself or through its immediate owner or highest-level owner) □ does, □ does not publicly disclose greenhouse gas emissions, i.e., makes available on a publicly accessible website the results of a greenhouse gas inventory, performed in accordance with an accounting standard with publicly available and consistently applied criteria, such as the Greenhouse Gas Protocol Corporate Standard.
(ii) The Offeror (itself or through its immediate owner or highest-level owner) □ does, □ does not publicly disclose a quantitative greenhouse gas emissions reduction goal, i.e., make available on a publicly accessible website a target to reduce absolute emissions or emissions intensity by a specific quantity or percentage.
(iii) A publicly accessible website includes the Offeror's own website or a recognized, third-party greenhouse gas emissions reporting program.
(3) If the Offeror checked "does" in paragraphs (t)(2)(i) or (t)(2)(ii) of this provision, respectively, the Offeror shall provide the publicly accessible website(s) where greenhouse gas emissions and/or reduction goals are reported:_____.
(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)

52.215-6 Place of Performance (Oct 1997)

(a) The offeror or respondent, in the performance of any contract resulting from this solicitation, ☐ intends, ☐ does not intend [check applicable block] to use one or more plants or facilities located at a different address from the address of the offeror or respondent as indicated in this proposal or response to request for information.

(b) If the offeror or respondent checks "intends" in paragraph (a) of this provision, it shall insert in the following spaces the required information:

Place of Performance (Street Address, City, State, County, ZIP Code)	Name and Address of Owner and Operator of the Plant or Facility if Other than Offeror or Respondent
-	-
-	-

52.219-1 Small Business Program Representations (Feb 2024)

(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.

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), 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 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, 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.

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

(1) Not less than 51 percent of which is owned 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 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) The North American Industry Classification System (NAICS) code for this acquisition is 561612

(2) The small business size standard is 17M.

(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 small-disadvantaged business concern as defined in 13 CFR 124.1001.

(3) [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 women-owned small business concern.

(4) 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: _.]

(5) 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: .]

(6) 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.

(7) SDVOSB concern. [Complete only if the offeror represented itself as a veteran-owned small business concern in paragraph (c)(6) of this provision.] The offeror represents as part of its offer that it ☐ is, ☐ is not an SDVOSB concern.

(8) SDVOSB joint venture eligible under the SDVOSB Program. [Complete only if the offeror represented itself as a SDVOSB concern in paragraph (c)(7) of this provision]. 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: _.]

(9) 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 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) 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, shall-

(1) Be punished by imposition of fine, imprisonment, or both;

(2) Be subject to administrative remedies, including suspension and debarment; and

(3) Be ineligible for participation in programs conducted under the authority of the Act.

52.223-22 Public Disclosure of Greenhouse Gas Emissions and Reduction Goals-Representation (DEC 2016)

(a)This representation shall be completed if the Offeror received $7.5 million or more in Federal contract awards in the prior Federal fiscal year. The representation is optional if the Offeror received less than $7.5 million in Federal contract awards in the prior Federal fiscal year.

(a) Representation. [Offeror is to check applicable blocks in paragraphs (1) and (2).]

(1) The Offeror (itself or through its immediate owner or highest-level owner) ☐ does, ☐ does not publicly disclose greenhouse gas emissions, i.e., make available on a publicly accessible website the results of a greenhouse gas inventory, performed in accordance with an accounting standard with publicly available and consistently applied criteria, such as the Greenhouse Gas Protocol Corporate Standard.

(2) The Offeror (itself or through its immediate owner or highest-level owner) ☐ does, ☐ does not publicly disclose a quantitative greenhouse gas emissions reduction goal, i.e., make available on a publicly available website a target to reduce absolute emissions or emissions intensity by a specific quantity or percentage.

(3) A publicly accessible website includes the Offeror's own website or a recognized, third- party greenhouse gas emissions reporting program.

(b) If the Offeror checked "does" in paragraphs (b)(1) or (b)(2) of this provision, respectively, the Offeror shall provide the publicly accessible website(s) where greenhouse gas emissions and/or reduction goals are reported: _.

3052.209-70 - Prohibition on Contracts with Corporate Expatriates (Jun 2006)

(a) Prohibitions.

Section 835 of the Homeland Security Act, 6 U.S.C. 395, prohibits the Department of Homeland Security from entering into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation as defined in this provision, or with any subsidiary of such an entity. The Secretary shall waive the prohibition with respect to any specific contract if the Secretary determines that the waiver is required in the interest of national security.

(b) Definitions.

As used in this provision: Expanded Affiliated Group means an affiliated group as defined in section 1504(a) of the Internal Revenue Code of 1986 (without regard to section 1504(b) of such Code), except that section 1504 of such Code shall be applied by substituting `more than 50 percent' for `at least 80 percent' each place it appears.

Foreign Incorporated Entity means any entity which is, or but for subsection (b) of section 835 of the Homeland Security Act, 6 U.S.C. 395, would be, treated as a foreign corporation for purposes of the Internal Revenue Code of 1986.

Inverted Domestic Corporation. A foreign incorporated entity shall be treated as an inverted domestic corporation if, pursuant to a plan (or a series of related transactions)—

(1) The entity completes the direct or indirect acquisition of substantially all of the properties held directly or indirectly by a domestic corporation or substantially all of the properties constituting a trade or business of a domestic partnership;

(2) After the acquisition at least 80 percent of the stock (by vote or value) of the entity is held—

(i) In the case of an acquisition with respect to a domestic corporation, by former shareholders of the domestic corporation by reason of holding stock in the domestic corporation; or

(ii) In the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and

(3) The expanded affiliated group which after the acquisition includes the entity does not have substantial business activities in the foreign country in which or under the law of which the entity
is created or organized when compared to the total business activities of such expanded affiliated group.

Person, domestic, and foreign have the meanings given such terms by paragraphs (1), (4),

and
(5) of section 7701(a) of the Internal Revenue Code of 1986, respectively.

(c) Special rules. The following definitions and special rules shall apply when determining whether a foreign incorporated entity should be treated as an inverted domestic corporation.

(1) Certain stock disregarded. For the purpose of treating a foreign incorporated entity as an inverted domestic corporation these shall not be taken into account in determining ownership:

(i) Stock held by members of the expanded affiliated group which includes the foreign incorporated entity; or

(ii) Stock of such entity which is sold in a public offering related to an acquisition described in section 835(b)(1) of the Homeland Security Act, 6 U.S.C. 395(b)(1).

(2) Plan deemed in certain cases. If a foreign incorporated entity acquires directly or indirectly substantially all of the properties of a domestic corporation or partnership during the 4-year period beginning on the date which is 2 years before the ownership requirements of subsection (b)(2) are met, such actions shall be treated as pursuant to a plan.

(3) *Certain transfers disregarded*. The transfer of properties or liabilities (including by contribution or distribution) shall be disregarded if such transfers are part of a plan a principal purpose of which is to avoid the purposes of this section.

(d) *Special rule for related partnerships*. For purposes of applying section 835(b) of the Homeland Security Act, 6 U.S.C. 395(b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the meaning of section 482 of the Internal Revenue Code of 1986) shall be treated as a partnership.

(e) Treatment of Certain Rights.

(1) Certain rights shall be treated as stocks to the extent necessary to reflect the present value of all equitable interests incident to the transaction, as follows:

(i) warrants;
(ii) options;
(iii) contracts to acquire stock;
(iv) convertible debt instruments; and
(v) others similar interests.

(2) Rights labeled as stocks shall not be treated as stocks whenever it is deemed appropriate to do so to reflect the present value of the transaction or to disregard

transactions whose recognition would defeat the purpose of Section 835.

(f) *Disclosure*. The offeror under this solicitation represents that [Check one]:

☐ it is not a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.1087003; ‘

☐ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.1087003, but it has submitted a request for waiver pursuant to 3009.108-7004, which has not been denied; or

☐ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.1087003, but it plans to submit a request for waiver pursuant to 3009.108-7004.

(g) A copy of the approved waiver, if a waiver has already been granted, or the waiver request, if a waiver has been applied for, shall be attached to the bid or proposal.

[END OF SECTION K]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION L:
INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS OR RESPONDENTS

L.1 PROVISIONS INCORPORATED BY REFERENCE

Number	Title	Date
52.204-7	System for Award Management (DEVIATION 25-19)	Aug 2025
52.215-1	Instructions to Offerors—Competitive Acquisition (DEVIATION 26-08)	Nov 2025

L.2 PROVISIONS INCORPORATED BY FULL TEXT

The following provisions include areas that must be completed by the offeror and submitted with its proposal.

52.216-1 Type of Contract (Apr 1984)

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

52.233-2 Service of Protest (Sept 2006)

(a) Protests, as defined in Part 33.104 of the Revolutionary FAR Overhaul (RFO), 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 by obtaining written and dated acknowledgment of receipt from Shane Crowl at Shane.Crowl@ice.dhs.gov.

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

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 address: https://www.acquisition.gov.

L.3 PROPOSAL INSTRUCTIONS

Offerors shall submit a proposal meeting the instructions below.

Note: This solicitation does not commit the government to pay any cost incurred in the submission of the offer or in making necessary studies or designs for the preparation thereof, nor to contract for services.

L.3.1 PROPOSAL VOLUMES AND PHASES

a. Offerors shall submit written proposals in the format and by the due date specified in this solicitation. Proposals that do not comply with these instructions may be considered non-responsive evaluated at a competitive disadvantage, or removed from competition.

b. The proposal shall consist of four separate volumes:

- Volume I – Administration
- Volume II – Written Proposal (Technical / Management, Past Performance)
- Volume III – Price/Cost Proposal

c. Each volume shall be complete and self-contained, so that evaluation of each factor can be accomplished independently.

d. Offerors shall clearly identify any proprietary information. The Government will handle proposal information in accordance with applicable law and regulations.

e. The Government may award a contract based on initial proposals received, without negotiations. Offerors are therefore urged to submit their best terms in the initial proposal.

L.3.2 PROPOSAL AND QUESTION SUBMISSION TIMES/DATES

a. Proposals shall be submitted electronically in the formats specified in the solicitation (e.g., searchable PDF, Excel for pricing templates).

b. Page limits (where stated) apply to the main narrative content and do not include required forms, cover pages, tables of contents, cross-reference matrices, or appendices expressly allowed.

c. Font shall be at least 11-point, with 1-inch margins, and pages shall be numbered.

d. The subject line for electronic submissions shall clearly identify the solicitation number and the offeror’s name.

As previously noted, the government intends to conduct this procurement through a single phased proposal submission and evaluation. Proposal and question submission times and dates are provided in the table below:

Event	Required Submission Date/Time
Solicitation Questions	**07/31/2026 / 2 p.m. Eastern**

Written Proposal Elements	**08/10/2026 / 5 p.m. Eastern**

Note: Please note, the above dates are subject to change.

L.3.3 PROPOSAL AND QUESTION SUBMISSION INSTRUCTIONS

1) **Questions:** All relevant questions related to this solicitation shall be submitted before the time and date specified above. Questions shall be submitted using Attachment 5 – Solicitation Question Template and instructions therein; questions submitted without this attachment may not be given consideration. Responses to all relevant questions submitted shall be provided together as an amendment to this solicitation as soon as possible after the time and date listed above.
2) **Proposal Submissions:** Offerors must submit a proposal volume in the required format before the time and date specified above.

Timely receipt of questions and proposals by the specified closing time and date is the sole responsibility of the offeror. Questions and proposals received after the time and date specified in this solicitation will be considered as late submissions and may be eliminated from further consideration. ICE shall not be responsible for late or non-delivery of offerors' proposals or questions due to information technology problems, servers or other technical issues. To ensure timely receipt of proposals and questions, offerors should NOT wait until the last moment to electronically submit. Proposals and questions submitted by facsimile, or any other means not described in this solicitation shall not be accepted.

Proposals and questions shall be submitted via email to **both** of following government personnel:

1) Shane Crowl; Shane.Crowl@ice.dhs.gov
2) Brittany Tobias; Brittany.Tobias@ice.dhs.gov

Note: Proposal and question submission emails must reference the solicitation number in its subject line.

L.4.5 PROPOSAL CONTENT

This section provides instructions for proposal content. It will be advantageous for offerors to present proposal elements in a clear, concise manner and in terms understandable to those who may be unfamiliar with the offeror's intentions and reasoning process. Responses should follow the PWS to the extent practicable. It should be noted that all elements of the offeror's submitted proposal that are accepted in response to this solicitation may be incorporated directly into the contract.

Proposal elements must be sufficiently detailed and complete to demonstrate an understanding of an ability to comply with the requirements of this solicitation. The proposal shall demonstrate such understanding and ability and should not contain superfluous material that is not related directly to this acquisition. General statements such as the offeror "can comply" or "will comply" with the requirements, that "standard procedures will be used", "well known techniques will be used", or that paraphrase the PWS in whole or part WILL NOT constitute compliance with the

requirements of this solicitation. Offerors must demonstrate capability of performing all tasks outlined in this solicitation, including the PWS and attachments.

Each proposal shall: (1) be specific and complete in every detail; (2) conform to all solicitation provisions, clauses, or other requirements; (3) be logically assembled, practical, legible, clear, concise, coherent; and indexed; and (4) contain appropriately numbered pages of each volume or part. Each volume shall be written on a stand-alone basis. Cross-referencing within a proposal volume is permitted where its use would conserve space without impairing clarity. Information required for each proposal evaluation factor, which is not found in its designated volume, will be assumed to have been omitted from the proposal.

The following provides detailed instructions for each volume/factor required under this solicitation.

1) Volume I: Administration

Volume I shall contain:

1) Cover letter, including:
    a. Offeror name, address, and UEI.
    b. Identification of the point of contact for the proposal (name, title, phone, email).
    c. Statement that the proposal is valid for at least [120] calendar days from the due date.
2) Completed representations and certifications (Section K), or confirmation that the offeror's online representations and certifications in SAM.gov are current as of the date of proposal submission.
3) Identification of any subcontractors, teaming partners, or joint-venture members, and their roles.

No evaluation factor is associated with Volume I, but omission of required administrative information may delay award.

2) **Volume II (Factors 1 and 2): Written Proposal**

Volume III consists of two parts:

- Part 1 – Technical / Management Approach (Factor 1)
- Part 2 – Past Performance (Factor 2)

3.1) Part 1 – Technical/Management Approach (Factor 1)

Technical: 15-page maximum; Management: 10-page maximum

Part 1 shall describe the offeror's Technical and Management Approach to performing the requirements of the PWS. At a minimum, the offeror shall address the following elements, in clearly labeled sections:

1. Understanding of the Requirement

    - A narrative explaining the offeror's understanding of the PWS requirements, including their understanding of the key elements required to provide safe, secure, humane, and expeditious transportation statewide under the 287(g) program.
    - Identification of critical success factors (e.g., statewide 30-minute average response time, 24/7/365 operations, surge capability, secure documentation, portal-based oversight) and how the proposed approach addresses them.

2. Web-Based Secure Portal

    - Description of the proposed contractor-hosted secure web portal and how it will address performance, scheduling, dispatch, reporting, and compliance with PWS requirements.
    - Discussion of core portal functions (GPS tracking, electronic Form G-391, transport and incident database, dashboards, data export, document repository, audit logging).
    - Explanation of how the portal will meet availability, performance, and security expectations, including the 99.9% uptime requirement (excluding approved maintenance).
    - Explanation of how the portal will support all required deliverables in PWS Section 12.0.

3. Fleet Plan

    - Description of the proposed fleet, including the minimum number of in-service vehicles, total number of vehicles, types/makes, model years, seating capacities, and major security modifications (e.g., partitions, cameras, panic/duress).
    - Explanation of how the fleet will meet or exceed PWS vehicle requirements and how the offeror will maintain at least 80% monthly operational readiness, including maintenance and sanitation approaches.

4. Staffing Plan

    - Description of the total workforce (prime and subcontractors) to be used to perform all PWS services, including transport officers, dispatchers, supervisors, key personnel, and support staff.
    - Explanation of how staffing will support continuous 24/7/365 operations, including shift structure, rotations, relief coverage, and surge staffing.
    - Description of pre-screening processes to identify and exclude candidates who are unlikely to meet ICE suitability requirements, and how the offeror will meet and maintain the minimum qualifications and licensing requirements in the PWS.
    - Describe how the offeror will monitor and maintain ongoing suitability compliance (including reinvestigation support and reporting of arrests or other reportable events), consistent with PWS Sections 6.5 and 6.7.

5. Operations Plan

- Description of the concept of operations for responding to 287(g) transport requests in all 254 Texas counties, including staging/loiter location strategy and dynamic deployment of transport teams.
- Approach for managing workload variability, long-distance transports, and changing pickup/drop-off locations while maintaining the statewide average 30-minute response time.
- Processes for communications between dispatch and field teams and for adapting to changes in volume, frequency, or geographic distribution of requests.
- Emergency Preparedness and Contingency Plan (EPCP): Describe the offeror's conceptual approach to developing and executing the EPCP required by PWS Section 11.0, including surge deployment (e.g., 50 additional teams within 24 hours), continuity of dispatch operations, and annual exercises (tabletop and functional).

6. Management Plan

- Management organization and structure, including an organizational chart with lines of authority and roles of key personnel (Program Manager, Deputy, Operations Manager, Training Manager, Fleet Manager, etc.).
- Description of subcontracting arrangements (if any) and how the prime will manage subcontractors to ensure uniform compliance with PWS requirements.
- Identification of major management risk areas and proposed strategies to reduce the probability and impact of those risks.
- Describe internal quality control and oversight mechanisms and how they integrate with the formal Quality Control Program (QCP) required by PWS Section 15.2, including planned inspections, audits, corrective action tracking, and use of customer feedback.

7. Transition-In Plan

- A schedule and narrative describing how the offeror will complete all tasks necessary to achieve Full Operational Capability within 120 calendar days of award.
- Identification of key milestones and tasks, including recruiting, hiring, security and suitability processing, training, obtaining licenses and permits, establishing facilities and staging areas, standing up the NCC-based dispatch center, and developing/testing/deploying the secure web portal.

Offerors should avoid marketing language and focus on specific, concrete approaches that demonstrate an understanding of and ability to meet PWS requirements.

3.2) Part 2 – Past Performance (Factor 2)

Offerors shall provide past performance information for no more than three contracts that are recent and relevant to this requirement. "Recent" is defined as services provided no later than 5 years from solicitation closing date. Page limit: No more than 3 pages per example, 9 pages maximum in total.

For each referenced contract, provide:

- Customer, contract number, contract type, and contract value.

- Period of performance and place of performance.
- Role of the offeror (prime, major subcontractor, joint venture member).
- Description of the work performed, including size, scope, and complexity.
- Explanation of why the effort is similar to this requirement (e.g., 24/7 operations, armed transport, statewide or multi-jurisdictional coverage, secure portal use).
- Customer point of contact (name, phone, email).

If subcontractors will perform major or critical aspects of the requirement, provide up to one recent and relevant reference for each such subcontractor. Each example will still count toward the three example maximum.

Offerors should also explain any significant past performance issues and address corrective actions taken. Contractors without a record of recent and relevant past performance, or for whom information is not available, will be evaluated in accordance with RFO 15.202 (c).

The Government may send Past Performance Questionnaires (PPQs) or may direct offerors to send blank PPQs to their references with instructions to return completed PPQs directly to the Government by the deadline specified in the solicitation.

3) **Volume III (Factor 3): Price**

a. Price Proposal

i. Page Limitation for Pricing Narrative: No page limitation.

ii. Format: See attachments referenced below; for pricing narrative, MS Word or PDF.

1. Pricing Template

- Offerors shall complete the Pricing Template (Attachment 2) for all specified CLINs and periods of performance (base and option periods). Offers must propose prices for all CLINs or their offer may be removed from competition.
- Offerors shall propose firm fixed prices for each CLIN consistent with their technical and staffing approaches.

2. Basis of Estimate (BOE)/Pricing Narrative

- For each CLIN, provide a Basis of Estimate sufficient to explain the assumptions underlying proposed prices, including labor categories, hours, rates, and major non-labor costs (e.g., vehicles, fuel, facilities), as directed in the Pricing Template.
- Clearly indicate which positions are to be fulfilled by subcontractors, if applicable.

3. Consistency with Technical Proposal

- Pricing shall be consistent with the technical, management, and staffing approaches described in Volume II.

- Any apparent inconsistency shall be explained in the price narrative; unexplained inconsistencies may indicate a lack of understanding and may adversely affect evaluation.

4. Contingency Pricing

- Offerors shall not include contingency allowances for cost increases that are subject to adjustment under applicable contract clauses (e.g., Service Contract Labor Standards price adjustments).

- Contractors shall not include contingency allowances to cover increased costs for which adjustments are provided under the RFO Clause 52.222-44 – Fair Labor Standards Act and Service Contract Labor Standards – Price Adjustment (Deviation Date).

- In addition to increases to wages and fringe benefits prescribed by a revised wage determination, including bona fide fringe benefits specifically called out in a collective bargaining agreement, ICE may consider increases to other direct costs brought about by the contractor's cost of compliance with the terms of a revised wage determination (e.g. state gross receipts tax). Any price adjustment request associated with such other direct cost(s) shall be supported by documentation demonstrating that a contingency covering an increase to the subject cost(s) was not included in the contractor's price proposal accepted by the Government at time of award.

- No contingency pricing is permitted. Any contingency pricing proposed may be grounds for removal from competition.

The minimum wage rates and fringe benefits applicable to the contract are outlined in the Department of Labor (DOL) prevailing wage determinations and/or predecessor contractor's CBA's. The applicable job classification under a DOL prevailing wage determination is **Detention Officer**. In the case of a CBA wage determination, the applicable job classification may be specified under a different title. In either case, the applicable job classification reflects the minimum wage rates and fringe benefits that the contractor must pay to all employees working under the contract. For purposes of proposal preparation, where a predecessor contractor's CBA applies, the minimum wages and fringe benefits of the predecessor contractor's CBA corresponding to the initial period of performance of this contract shall be regarded as applicable to all additional period of performance under this contract.

To ensure a fair procurement process, the Government instructs all Offerors to base pricing for all collective bargaining agreement labor categories on the entry level position with no seniority or leave accrual. The awarded contractor shall submit a request for equitable adjustment, based on actual staffing levels, once the seniority list is provided after award.

4) **Additional Items to Provide with Price Proposal**
   i. Page Limitation: No page limitations.
   ii. Format: MS Word or PDF.

1. **Legal Offer Letter:** The legal offer letter shall reference the solicitation number

and acknowledge that it transmits an offer in response to the solicitation. It shall identify all enclosures being transmitted as part of the proposal and state proposal validity through at least 3 months after the proposal submission deadline.

2. **Small Business Individual Subcontracting Plan:** In accordance with RFO Clause 52.219-9, Small Business Subcontracting Plan, offerors who do not qualify as small businesses (i.e., those companies described as "other than small businesses") shall submit an individual subcontracting plan (Factor 4) which includes all the required information in accordance with RFO 52.219-9(d). The following small business subcontracting goals may be considered when developing a subcontracting plan in response to this solicitation.

Small Business Subcontracting Goals	
Concern Type	**Goal (Percentage)**
Small Business	39%
Small Disadvantaged Business	5%
Historically Underutilized Business Zone Small Business	3%
Service-Disabled Veteran-Owned Small Business	5%
Women-Owned Small Business	5%

If an offeror plans on entering into a teaming arrangement or joint venture to perform the services required in this solicitation, then the offeror shall provide a copy of the teaming arrangement or joint venture documents outlining the structure and arrangement of the arrangement/venture.

3. **Provision and Clause Fill-in:**
Offerors must complete any provision and/or clause requiring fill-in included in Sections I and K. In addition, offerors must include one (1) of the following two (2) statements within this volume regarding the terms and conditions applicable to this solicitation:

"The terms and conditions included in this solicitation are acceptable to be included in the award document without modification, deletion, or addition."

OR

"The terms and conditions included in this solicitation are acceptable to be included in the award document with the exception, deletion, or addition of the following: [offeror shall list exception(s) and rationale for the exception(s)]."

Note 1: Taking an exception to a term or condition may render the proposal unacceptable. In addition, any exception taken to any other requirement in this solicitation is invalid and will not be considered.

Note 2: Any proprietary data included in this volume shall be clearly identified. Each page that contains proprietary data shall be marked CONTRACTOR PROPRIETARY at the top and bottom of the page.

4. Proof of DHS Mentor-Protégé program (if applicable)

[END OF SECTION L]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION M:
EVALUATION FACTORS FOR AWARD

M.1 CLAUSES INCORPORATED BY REFERENCE

Number	Title	Date
52.217-5	Evaluations of Options (DEVIATION 25-36)	Nov 25

M.2 CLAUSES INCORPORATED BY FULL TEXT

None.

M.3 GENERAL

All submissions should be identical to, or conform closely to, the terms set forth in this solicitation. Proposals must: (1) be specific and complete in every detail; (2) be logically assembled, practical, legible, clear, concise, coherent; and indexed (cross-indexed, where appropriate); and (3) contain appropriately numbered pages of each volume or part. Proposals must clearly demonstrate how the offeror intends to accomplish the solicitation requirements and must include convincing rationale and substantiation of all claims. Offerors shall assume that the government has no prior knowledge of their experience and will base its evaluation on the information presented in the offerors' proposal.

The proposals shall be submitted in accordance with the instructions in Section L. An offer may be rejected as deficient if the CO determines that the proposal does not comply with the solicitation instructions. In addition, the government may: (1) reject the submittal if such action is in the public interest; (2) accept other than the lowest price submittal; and/or (3) waive informalities and minor irregularities in offers received.

M.4 RESERVED

M.5 AWARD SELECTION – BEST VALUE

The Government intends to award a contract to the contractor whose proposal for the services described herein conforms to the solicitation and represents the overall best value to ICE. The Government intends to award by means of a best value tradeoff approach. The best value tradeoff approach is a method of selecting the proposals that represents the best value to the Government, based on the evaluation of each proposal and conducting tradeoffs between price and non-price factors. In accordance with RFO 15.205, the government will utilize the tradeoff source selection process to obtain best value. A tradeoff process is appropriate when it may be in the best interest of the government to consider award to other than the lowest priced offeror or other than the highest technically rated offeror.

The Government intends to evaluate proposals and award upon initial proposals submitted, reserving the right to award without negotiations. Therefore, the offeror's initial proposal submittal should contain the offeror's best terms. However, the government reserves the right

to enter into negotiations, establish a competitive range, and if necessary, request Final Proposal Revisions for all Volumes from contractors. At the conclusion of negotiations (if applicable), all offerors still within the competitive range shall be given the opportunity to submit a final proposal revision.

The Government will evaluate proposals in accordance with the requirements of RFO Subpart 15.2, "Evaluation and Award." Offerors must recognize that the initial evaluation of proposals and the determination of the competitive range, if any, will be made upon a review of the proposals only, plus some independent investigations that may be made with regard to Past Performance. If written or oral negotiations are conducted, the Government may seek revised proposals from Offerors within the competitive range

The Source Selection Authority's (SSA) decision shall be based on a comparative assessment of proposals against all source selection criteria in the solicitation. While the SSA may use reports and analyses prepared by others, the source selection decision shall represent the SSA's independent judgment. The government intends to award a contract resulting from this solicitation to the responsible offeror(s) whose proposal represents the best value after evaluation in accordance with the criteria set forth in the solicitation.

M.6 EVALUATION FACTORS

There are three (3) evaluation factors in total for this procurement. These factors are as follows:

1) Evaluation Factor 1: Technical / Management Approach (Volume II)
2) Evaluation Factor 2: Past Performance (Volume II)
3) Evaluation Factor 3: Price Proposal (Volume III)

Specific information regarding each factor is provided below.

1) Factor 1: Technical Approach / Management Approach (Volume III)

The Government will evaluate whether the offeror's proposed approach demonstrates an understanding of the requirement and the feasibility and effectiveness of its plan to perform the work by evaluating the following seven elements, focusing the their specific evaluation discriminators:

1) Understanding of the Requirement:

- Clearly explains the mission, operating environment, and key performance drivers (for example, statewide 30 minute average response, 24/7/365 operations, armed transport, secure chain of custody documentation).
- Connects those drivers to specific design choices in its concept of operations, staffing, fleet, and portal.
- Recognizes major risks and constraints inherent in statewide 287(g) transportation and addresses them in a realistic manner.

NOTE: Narratives that simply restate the PWS without demonstrating insights, tradeoffs, or an appreciation of operational risk will be rated less favorably.

2) Web-Based Secure Portal:

- Functionally robust: provides required capabilities such as real-time or near real-time GPS tracking, electronic Form G-391, transport and incident database, dashboards, queries, reporting, document storage, and audit logging.
- Operationally usable: supports dispatchers, ICE users, and management with clear workflows, reporting, and dashboards that enable oversight and performance management.
- Reliable and secure: realistically capable of meeting availability expectations (for example, 99.9 percent uptime), with appropriate access control, encryption, logging, and data protection measures.

NOTE: The Government will assign higher confidence where the offeror presents a mature, well-described system or a credible enhancement of an existing solution with proven performance on similar contracts. Proposals that are overly conceptual, lack detail, or appear difficult to implement or sustain will reduce confidence.

2) Fleet Plan:

- Is sized appropriately for the anticipated workload and geography, including sufficient in service vehicles to support statewide operations and surge.
- Uses vehicle types and configurations that align with PWS requirements and operational needs (for example, seating capacity, security partitions, camera systems, duress capabilities).
- Includes realistic maintenance and sanitation strategies to meet or exceed the required operational readiness rate and applicable health standards.

NOTE: Plans that show a clear linkage between mission demand, modeling or analysis of fleet needs, and specific readiness strategies will be evaluated more favorably. Fleets that appear undersized, outdated, or unsupported by credible maintenance plans may be assessed as higher risk.

3) Staffing Plan:

- Provides sufficient numbers and types of personnel to support 24/7/365 statewide coverage, with clear coverage patterns for normal operations and surge.
- Aligns staffing levels with the proposed concept of operations, response time expectations, and training/qualification requirements.
- Includes practical prescreening, hiring, retention, and succession strategies to sustain qualified staff over time.
- Demonstrates a clear approach to maintaining required licenses, clearances, and training.

NOTE: Staffing approaches that are quantitatively and qualitatively consistent with the workload, and that demonstrate realistic coverage and contingency planning, will be viewed as strengths. Plans that lack specificity, rely on optimistic assumptions, or do not credibly account for suitability, licensing, and training requirements will reduce confidence.

4) Operations Plan:

- Coherent statewide concept of operations: how vehicles and teams are staged, redeployed, and managed across all 254 Texas counties.

- Practical methods to achieve and sustain the 30 minute statewide average response time, including how the offeror will monitor and adjust staging.
- Effective dispatch and communication processes, including but not limited to handling long distance trips, overlapping requests, and changes in pickup and drop off locations.
- Flexibility to absorb changes in volume, locations, or participating jurisdictions with minimal disruption and efficient use of resources.

NOTE: Plans that show detailed, data driven staging and dispatch models, clear rules for prioritization, and realistic surge concepts will be rated more favorably. High level or generic descriptions with little indication of how statewide performance will actually be achieved will be rated lower.

5) Management Plan:

- Roles, responsibilities, and lines of authority are clearly defined and appropriate for the scope and complexity of the work.
- The prime contractor's approach to managing subcontractors will ensure consistent compliance with security, training, reporting, and performance requirements.
- Identified management risks (for example, staffing shortfalls, fleet readiness, portal availability, compliance issues) have realistic and proactive mitigation strategies.
- Internal quality control and oversight mechanisms are specific, tied to measurable outcomes, and integrated with the Quality Control Program required by the PWS.

NOTE: Proposals that offer a clear, disciplined management structure with defined processes for monitoring, correcting, and reporting performance will be viewed more favorably than those that rely primarily on generic management statements.

6) Transition In Plan:

- Provides a credible schedule and sequencing of tasks to reach FOC within 120 calendar days.
- Identifies critical path activities (for example, hiring, clearances, fleet acquisition and outfitting, facilities, portal deployment) and accounts for their dependencies and lead times.
- Includes contingency approaches for common transition risks, such as delays in hiring, licensing, or vehicle delivery.

NOTE: Transition plans that show realistic durations, clear milestones, and contingency measures will be rated higher. Plans that assume overly optimistic timelines, omit key steps, or lack contingency planning will reduce confidence.

For Factor 1, the government will assign a confidence rating based upon the below definitions:

High Confidence	The government has high confidence that the offeror understands the requirement, proposes a sound approach and will be successful in performing the requirement with little or no government intervention.

Some Confidence	The government has some confidence that the offeror understands the requirement, proposes a sound approach, and will be successful in performing the requirement with some government intervention.
Low Confidence	The government has low confidence that the offeror understands the requirement, proposes a sound approach, and will be successful in performing the requirement even with government intervention.

3) Factor 2: Past Performance (Volume II)

The Government will evaluate:

- Quality of performance (meeting schedule, response time, safety, and reporting requirements).
- Management of staffing, training, and surge requirements in 24/7 environments.
- Compliance with security, suitability, and PREA requirements and handling of any incidents, escapes, or serious safety events.
- Responsiveness to issues and effectiveness of corrective actions.

The Government may use information provided by the offeror, information obtained from Government databases (e.g., CPARS), and other sources. Offerors with no recent and relevant past performance, or for whom no information is available, will receive a neutral rating (no positive or negative impact).

Offerors are cautioned to ensure the completeness and accuracy of past performance information. The Government may consider adverse past performance information even if it is not identified by the offeror.

When applying the definitions below to arrive at a confidence rating, the government will evaluate each Offeror's relevant past performance (e.g., recency, relevancy, scope, and complexity) to assess the Offeror's overall confidence rating assigned. The past performance evaluation is an assessment of the Government's confidence in the Offeror's ability to successfully perform the solicitation requirements. Past Performance shall be evaluated for each Offeror using the following levels of confidence ratings:

High Confidence	Based on the Offeror's recent (NLT 5 years from solicitation closing date), relevant (similar in size, scope and complexity to this effort), and performance record, the Government has a high expectation that the Offeror will successfully perform.
Some Confidence	Based on the Offeror's recent (NLT 5 years from solicitation closing date), relevant (similar size, scope and complexity to this effort), and performance record, the Government has a reasonable expectation that the Offeror will successfully perform.
	Based on the Offeror's recent (NLT 5 years from solicitation closing date), relevant (similar in size, scope and complexity to this effort), and

Low Confidence	performance record, the Government has a low expectation that the Offeror will successfully perform.
Unknown Confidence (Neutral)	The Offeror does not have recent (NLT 5 years from solicitation closing date), relevant (similar in size, scope and complexity to this effort), or any performance record; or the Offeror's performance record is so sparse, a meaningful confidence rating cannot be reasonably assigned.

4) Factor 3: Price/Cost Proposal (Volume III)

This factor is used to assess what each offeror's proposal will cost the government should it be selected for award. A price analysis will be conducted to assess the reasonableness of the proposed prices. This factor will not be assigned a confidence level rating.

The government will also evaluate the additional items provided with the price proposal including the legal offer letter, small business individual subcontracting plan, and provision and clause fill-ins. Failure to submit these items may make the offeror ineligible for award.

The Government may conduct a price realism analysis. To the extent price realism analysis is performed, the Government will:

- Review labor mixes, hours, and major non-labor cost elements (for example, vehicles, fuel, facilities) for consistency with the technical, management, and staffing approaches.
- Identify apparent underpricing or over-pricing that may indicate performance risk, such as insufficient staffing to meet response times or inadequate resources for fleet readiness.

Any realism analysis will be used to assess performance risk and understanding, not to adjust the offeror's proposed prices.

The Government may evaluate proposals for unbalanced pricing. An offer may be considered unacceptable if materially unbalanced prices pose an unacceptable risk to the Government.

Offerors shall not include contingency allowances for cost increases that are subject to adjustment under applicable clauses. Inclusion of contingency pricing may be grounds for removing the proposal from further consideration.

The Government may review Basis of Estimate (BOE) information to verify that the proposed prices are based on reasonable assumptions consistent with the described technical and staffing approaches. Significant omissions or inconsistencies between the BOE and other proposal volumes may adversely affect the evaluation under this factor and may inform the assessment of other factors.

Note 1: The government will review the small business subcontracting plan of the apparent awardee. The small business subcontracting plan shall be finalized prior to contract award and will be made part of a resulting contract. Failure to submit and finalize a small business subcontracting plan shall make the offeror ineligible for award of a contact.

Note 2: The government will review submitted evidence of an established DHS Mentor-Protégé program.

M.7 DEFINITION OF TERMS

The government will consider relative strengths, weaknesses, significant weaknesses, and deficiencies, when conducting its evaluation and utilizing the definitions below.

Strength	A material aspect of the proposal that increases the government's confidence of successful contract performance.
Risk	A flaw in the proposal that increases the risk of unsuccessful contract performance.
Significant Weakness	A flaw in the proposal that appreciably increases the risk of unsuccessful contract performance.
Deficiency	A material failure of a proposal to meet a government requirement or a combination of significant weaknesses in a proposal that increases the risk of unsuccessful contract performance to an unacceptable level.

M.8 METHODOLOGY OF EVALUATION

Each proposal will be evaluated based on effectiveness, expected outcomes, sound business practices, demonstrated understanding of all elements of the technical requirements, and fair and reasonable pricing. Proposals which fail to meet solicitation requirements or do not demonstrate a technical understanding of the requirements or schedule may be deemed to be reflective of an inherent lack of technical competence, or indicative of a failure to comprehend the complexity and risks of the proposed work and may be grounds for rejection. The SSA may determine that a superior solution/approach, as determined through the evaluation factors, merits a higher price, and therefore represents the best value to the Government. The SSA, using sound business judgment, will base the selection decision on an integrated assessment of the Offeror's relative capability as measured against the evaluation factors.

M.9 RELATIVE IMPORTANCE OF FACTORS

For purposes of this requirement, the following is the relative importance of the factors, listed in descending order of importance: Factor 1 (Technical/Management), Factor 2 (Past Performance), and Factor 3 (Price). The non-price factors, when combined, are more important than price.

The government will not make an award at a significantly higher overall price to achieve only slightly superior technical capability. As the technical merits of competing proposals become comparable, price will become more important in tradeoff decisions. Notwithstanding the above, proposals may be removed from competition if they receive an overall "Low Confidence" rating in non-price Factors 1 or 2.

M.10 RESPONSIBLE PROSPECTIVE CONTRACTORS

In addition to the evaluation methodology outlined in this solicitation, an offeror must also be found responsible by the CO prior to the award of any resultant contract. This responsibility determination will only be performed on the apparent awardee prior to award. At a minimum, to be determined responsible a prospective contractor must:

a) Have adequate financial resources to perform the contract, or the ability to obtain those resources.
b) Be able to comply with the required or proposed performance schedule taking into consideration all other business commitments.
c) Have a satisfactory performance record
d) Have a satisfactory record of integrity and business ethics.
e) Have the necessary organization, experience, accounting and operational controls.
f) Have the necessary production, construction, and technical equipment and facilities, or the ability to obtain them.
g) Be otherwise qualified and eligible to receive an award under applicable laws and regulations.

[END OF SECTION M]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]