SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

NOTE: OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, AND 30.

1. REQUISITION NUMBER

2. CONTRACT NUMBER

3. AWARD/EFFECTIVE DATE

4. ORDER NUMBER

5. SOLICITATION NUMBER
70SBUR26Q00000188

6. SOLICITATION ISSUE DATE
08/12/2026

7. FOR SOLICITATION INFORMATION CALL:

a. NAME
Vanh Phun

b. TELEPHONE NUMBER *(No collect calls)*
802-288-7933

8. OFFER DUE DATE/ LOCAL TIME
08/17/2026 1700 ET

9. ISSUED BY CODE 70SBUR

DHS / USCIS
Office of Contracting
124 Leroy Road
Williston VT 05495

10. THIS ACQUISITION IS
- [ ] UNRESTRICTED OR
- [x] SET ASIDE: 100.00 % FOR:
- [x] SMALL BUSINESS
- [ ] HUBZONE SMALL BUSINESS
- [ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS (SDVOSB)
- [ ] WOMEN-OWNED SMALL BUSINESS (WOSB)
- [ ] ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB)
- [ ] 8(A)

NORTH AMERICAN INDUSTRY CLASSIFICATION STANDARD (NAICS): 561611

SIZE STANDARD: $25

11. DELIVERY FOR FREE ON BOARD (FOB) DESTINATION UNLESS BLOCK IS MARKED
- [x] SEE SCHEDULE

12. DISCOUNT TERMS

13a. THIS CONTRACT IS A RATED ORDER UNDER THE DEFENSE PRIORITIES AND ALLOCATIONS SYSTEM - DPAS (15 CFR 700)
- [ ]

13b. RATING

14. METHOD OF SOLICITATION
- [x] REQUEST FOR QUOTE (RFQ)
- [ ] INVITATION FOR BID (IFB)
- [ ] REQUEST FOR PROPOSAL (RFP)

15. DELIVER TO CODE

16. ADMINISTERED BY CODE 70SBUR

DHS / USCIS
Office of Contracting
124 Leroy Road
Williston VT 05495

17a. CONTRACTOR/ OFFEROR CODE FACILITY CODE

TELEPHONE NUMBER

18a. PAYMENT WILL BE MADE BY CODE

- [ ] 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

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

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Period of Performance: 09/30/2026 to 09/29/2027				
0001	Scientific and Program Support Services	1	LO		
	Continued...				
	(Use Reverse and/or Attach Additional Sheets as Necessary)				

25. ACCOUNTING AND APPROPRIATION DATA

26. TOTAL AWARD AMOUNT *(For Government Use Only)*

- [ ] 27a. SOLICITATION INCORPORATES BY REFERENCE (FEDERAL ACQUISITION REGULATION) FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED
- [ ] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED

- [x] 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED

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

30a. SIGNATURE OF OFFEROR/CONTRACTOR

31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*

30b. NAME AND TITLE OF SIGNER *(Type or print)*

30c. DATE SIGNED

31b. NAME OF CONTRACTING OFFICER *(Type or print)*
Gregory Forrest

31c. DATE SIGNED

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Product/Service Code: R499				
0002	Other Direct Costs: Travel This is a NOT-TO-EXCEED Line Item with a not-to-exceed ceiling of $18,310.00. Product/Service Code: R499				
0003	Expert Witness Testimony Product/Service Code: R499	1	LO		
1001	Expert Witness Testimony (Option Line Item) 09/29/2027 Product/Service Code: R499 Period of Performance: 09/30/2027 to 09/29/2028	1	LO		
1002	Other Direct Costs: Travel This is a NOT-TO-EXCEED Line Item with a not-to-exceed ceiling of $48,400.00. (Option Line Item) 09/29/2027 Product/Service Code: R499 Period of Performance: 09/30/2027 to 09/29/2028				

Continued...

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE 32g. EMAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT	37. CHECK NUMBER
☐ PARTIAL ☐ FINAL			☐ COMPLETE ☐ PARTIAL ☐ FINAL	

STOCK RECORD (S/R)		40. PAID BY
38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*	
		42c. DATE RECEIVED *(MM/DD/YYYY)*	42d. TOTAL CONTAINERS

NAME OF OFFEROR OR CONTRACTOR

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
1003	Quantity Option Additional Scientific and Program Support Services (Option Line Item) 09/29/2027 Product/Service Code: R499 Period of Performance: 09/30/2027 to 09/29/2028	1	LO		
2001	Expert Witness Testimony (Option Line Item) 09/29/2028 Product/Service Code: R499 Period of Performance: 09/30/2028 to 09/29/2029	1	LO		
2002	Other Direct Costs: Travel This is a NOT-TO-EXCEED Line Item with a not-to-exceed ceiling of $99,300.00. (Option Line Item) 09/29/2028 Product/Service Code: R499 Period of Performance: 09/30/2028 to 09/29/2029				
3001	Expert Witness Testimony (Option Line Item) 09/29/2029 Product/Service Code: R499 Period of Performance: 09/30/2029 to 09/29/2030	1	LO		
3002	Other Direct Costs: Travel This is a NOT-TO-EXCEED Line Item with a not-to-exceed ceiling of $101,800.00 (Option Line Item) 09/29/2029 Product/Service Code: R499 Period of Performance: 09/30/2029 to 09/29/2030 SOLICITATION DOCUMENTS: Continued...				

NAME OF OFFEROR OR CONTRACTOR

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	PART I: SCHEDULE (SF1449) PART II: SOLICITATION CLAUSES PART III: LIST OF ATTACHMENTS A. STATEMENT OF WORK (SOW) B. SECURITY REQUIREMENT PART IV: SOLICITATION PROVISIONS/INSTRUCTIONS/EVALUATION				

Part II – Solicitation Clauses/Terms and Conditions

Federal Acquisition Regulation (FAR) Clauses Incorporated by Reference

52.252-2	**Clauses Incorporated by Reference**	**FEB 1998**

This contract incorporates one of 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: FAR & HSAR Clauses: https://www.acquisition.gov

(End of clause)

FAR Clauses Incorporated by Reference

52.203-6	**Restrictions on Subcontractor Sales to the Government**	**JUN 2020**
52.203-17	**Contractor Employee Whistleblower**	**NOV 2023**
52.203-12	**Limitation on Payments to Influence Certain Federal Transactions**	**JUN 2020**
52.203-19	**Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements**	**JAN 2017**
52.204-9	**Personal Identify Verification of Contractor Personnel**	**JAN 2011**
52.204-19	**Incorporation by Reference of Representations and Certifications**	**DEC 2014**
52.209-6	**Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended, Proposed for Debarment, or Voluntarily Excluded (NOV 2025) (DEVIATION 25-27)**	**NOV 2025**
52.209-9	**Updates of Publicly Available Information Regarding Responsibility Matters (NOV 2025) (DEVIATION 25-27)**	**NOV 2025**
52.209-10	**Prohibition on Contracting with Inverted Domestic Corporations (NOV 2025) (DEVIATION 25-27)**	**NOV 2025**
52.212-4	**Contract Terms and Conditions – Commercial Products and Commercial Services (AUG 2025) (DEVIATION 25-21)**	**NOV 2025**
52.219-6	**Notice of Total Small Business Set-Aside (OCT 2025) (DEVIATION 26-03)**	**OCT 2025**
52.219-8	**Utilization of Small Business Concern (OCT 2025) (DEVIATION 26-03)**	**OCT 2025**
52.219-14	**Limitations on Subcontracting (OCT 2025) (DEVIATION 26-03)**	**OCT 2025**
52.222-35	**Equal Opportunity for Veterans (OCT 2025) (DEVIATION 26-10)**	**OCT 2025**
52.222-36	**Equal Opportunity for Workers with Disabilities (OCT 2025) (DEVIATION 26-10)**	**OCT 2025**

52.222-37	**Employment Reports on Veterans (OCT 2025) (DEVIATION 26-10)**	**OCT 2025**
52.222-40	**Notification of Employee Rights Under the National Labor Relations Act**	**DEC 2010**
52.222-50	**Combating Trafficking in Persons**	**NOV 2021**
52.222-54	**Employment Eligibility Verification (OCT 2025) (DEVIATION 26-10)**	**OCT 2025**
52.226-8	**Encouraging Contractor Policies to Ban Text Messing While Driving**	**MAY 2024**
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 (AUG 2025) (DEVIATION 25-25)**	**AUG 2025**
52.233-4	**Applicable Law for Breach of Contract Claim (AUG 2025) (DEVIATION 25-25)**	**AUG 2025**

FAR Clauses Referenced in Full Text

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

(End of clause)

52.204-13	**System for Award Management Maintenance (AUG 2025) (DEVIATION 25-19)**	**NOV 2025**

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

Commercial and Government Entity 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 (referred to as "CAGE code"); or

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

Unique Entity Identifier (UEI) means an identifier used to identify a specific commercial, nonprofit, or Government entity.

(b) *Active Registration*.

(1) The Contractor shall maintain an active Federal Government contracts registration in the System for Award Management (SAM) at https://www.sam.gov during contract performance and through final payment under this contract. To maintain an active registration in SAM, the Contractor shall review at least annually its registration in SAM and validate that the information is current, accurate, and complete.

(2) The Contractor is responsible for the currency, accuracy, and completeness of the information provided within SAM, and for any liability resulting from the Government's reliance on inaccurate or incomplete information. Updating SAM does not alter the terms and conditions of this contract and is not a substitute for a properly executed contractual document.

(c) *Novation and change-of-name agreements*.

(1) If the Contractor has legally changed its business name or "doing business as" name (whichever is shown on the contract), or has transferred the assets used to perform the contract, but has not competed the necessary requirements regarding novation and change-of-name agreements in part 42 of the Federal Acquisition Regulation (FAR), the Contractor shall provide the responsible Contracting Officer a minimum of one business day's written notification of its intention to –

(i) Change the legal business name in SAM;

(ii) Comply with the requirements of FAR part 42; and

(iii) Agree in writing to the timeline and procedures specified by the responsible Contracting Officer. The Contractor shall provide with its written notification sufficient documentation to support the legal changed name.

(2) If the Contractor fails to comply with the requirements of paragraph (c)(1) of this clause, or fails to perform the agreement at paragraph (c)(1)(iii) of this clause, and, in the absence of a properly executed novation or change-of-name agreement, the SAM information that shows the Contractor to be other than the Contractor indicated in the contract will be considered to be incorrect information within the meaning of the "Suspension of Payment" paragraph of the electronic funds transfer (EFT) clause of this contract.

(d) *Assignees*.

(1) The Contractor shall not change the legal business name of address for EFT payments or manual payments, as appropriate, in the SAM record to reflect an assignee for the purpose of assignment of claims (see FAR part 32). Assignees shall be separately registered in SAM.

(2) Information provided to the Contractor's SAM record that indicates payments, including those made by EFT, to an ultimate recipient other than that Contractor will be incorrect information within the meaning of the "Suspension of Payment" paragraph of the EFT clause of this contract.

(e) *Unique entity identifier (UEI)*. The Contractor shall ensure that its UEI is maintained throughout the life of the contract.

(f) *Commercial and Government Entity (CAGE) code*. The Contractor shall ensure that the CAGE code is maintained throughout the life of the contact. To update a CAGE code, the Contractor shall initiate the change by updating its SAM registration.

(g) *Communicating changes*. The Contractor shall communicate any change to its UEI or CAGE code to the Contracting Officer within 30 days after the change, so a modification can be issued to update the UEI or CAGE code on this contract. A change in the UEI does not necessarily require a novation.

(End of clause)

52.217-7	Option for Increased Quantity – Separately Priced Line Item (APR 2026) (DEVIATION 24-05, Revision 1)	APR 2026

The Government may require the delivery of the numbered line item, identified in the Schedule as an option item, in the quantity and at the price stated in the Schedule. The Contracting Officer may exercise the option by written notice to the Contractor within 10 calendar days before additional services commence. Performance of added services shall comply with the requirements identified in the Schedule.

(End of clause)

52.217-9	Option to Extend the Term of the Contract	MAR 2000

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

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 48 months (Base + three (3) one-year Option)

(End of clause)

52.222-90	Addressing DEI Discrimination by Federal Contractors (APR 2026) (DEVIATION 26-10, Revision 2)	APR 2026

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

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

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

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

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

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

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

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

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

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

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

(End of clause)

52.224-3	**Privacy Training – Alternate I (DEVIATION 17-03, Revision 2)**	**MAR 2026**

(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 24.3).

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to the 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 or records.

(End of clause)

52.240-91	**Security Prohibitions and Exclusions (AUG 2025) (DEVIATION 25-23)**	**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 any 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 purposes 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 reason 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 par 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 of 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 order 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 products;

(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 Bureaus 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 a telephone provide 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 of 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 on 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.

Service 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, or 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 space 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 Consolidation 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) 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

(ii) 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 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 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 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 require, for use in the performance of this contract, any supplies or services if any proclamation, Executive order, or statue 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/fiancial-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 to 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) Contractors are prohibited from providing or using as a 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).

Yes ___ No ___ DHDS FASCSA Order

Yes ___ No ___ DoD FASCSA Order

Yes ___ No ___ DNI FASCSA Order

(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 inquiring*. 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 prohibitive products and services*. For Federal Supply Schedules, Governmentwide acquisition contracts, multi-agency contracts or any 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 identified 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 (including 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 distributors 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 identified 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 Representative, and the Enterprise Security Operations Center (SOC)

at NDAA_Incidents@hq.dhs.gov, with the required information in the body of the email. In the case of 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 Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite 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 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 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 order report*.

(1) During contract performance, the Contractor shall review SAM at least once every three month, 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 with 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)

52.244-6	**Subcontracts for Commercial Products and Commercial Services (APR 2026) (DEVIATION 26-10, Revision 2)**	**APR 2026**

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

Commercial product, commercial service and nondevelopmental item have the meanings contained in Federal Acquisition Regulation (FAR) 2.101.

Subcontract has the meaning at FAR 44.401

(b) *Requirements*.

(1) To the maximum extent practicable, the Contractor shall incorporate, and require its subcontractors at all ties to incorporate, commercial products, commercial services, or non-developmental items as components of items to be supplied under this contract.

(2) If a clause in the following table is included in the contract, the Contractor shall insert the clause in subcontracts for commercial products or commercial services and must flow down the requirements of the clause to subcontracts as indicated in the specific clause:

Number	Title	Date
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
52.219-8*	Utilization of Small Business Concerns	JAN 2025
52.222-35	Equal Opportunity for Veterans	JUN 2020
52.222-36	Equal Opportunity for Workers with Disabilities	JUN 2020
52.222-37	Employment Reports on Veterans	JUN 2020
52.222-40	Notification of Employee Rights Under the National Labor Relations Act	DEC 2010
52.222-41	Service Contract Labor Standards	AUG 2018
52.222-50	Combating Trafficking in Persons	NOV 2021
52.222-50 With Alt I	Combating Trafficking in Person, with its Alternate I	MAY 2015
52.222-51	Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment – Requirements	MAY 2014
52.222-53	Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services – Requirements	MAY 2014
52.222-54	Employment Eligibility Verification	JAN 2025
52.222-62	Paid Sick Leave Under Executive Order 13706	JAN 2022
52.224-3	Privacy Training	JAN 2017
52.224-3 With Alt I	Privacy Training, with Alternate I	JAN 2017
52.225-26	Contractors Performing Private Security Functions Outside the United States	OCT 2016
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	MAR 2023
52.240-3	Security Prohibitions and Exclusions	DATE
52.240-3 With Alt I	Security Prohibitions and Exclusions, with its Alternate I	DATE
52.240-4	Security Requirements	DATE
52.240-4 With Alt II	Security Requirements, with its Alternate II	DATE
52.247-64	Preference for Privately Owned U.S.-Flag Commercial Vessels	NOV 2021
52.222-90	Addressing DEI Discrimination by Federal Contractors	APR 2026

* Include only if the subcontract offers further subcontracting opportunities. If the subcontract (except subcontractors to small businesses concerns) exceeds the applicable threshold specified in FAR 19.702(a) on the date of subcontract award, the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(c) *Subcontracts*. The Contractor shall include the terms of this clause, including this paragraph (c), in subcontracts awarded under this contract.

(End of clause)

HSAR Clauses Incorporated By Full Text

3052.212-70	**Contract Terms and Conditions Applicable to DHS Acquisition of Commercial Items (HSAR DEVIATION 25-09)**	**JUL 2023**

The Contractor agrees to comply with any provisions 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 applicable regulation cited on the date the solicitation is issued applies unless otherwise stated herein. The following provisions and clauses are incorporated by reference:

(b) *Clauses*.

_X_ 3052.203-70 Instructions for Contractor Disclosure of Violations.
_X_ 3052.205-70 Advertisement, Publicizing Awards, and Releases.
_X_ 3052.209-72 Organizational Conflicts of Interest
_X_ 3052.242-72 Contracting Officer's Representative

(End of clause)

3052.222-70	**Strikes or Picketing Affecting Timely Completion of the Contract Work**	**DEC 2003**

Notwithstanding any other provision hereof, the Contractor is responsible for delays arising out of labor disputes, including but not limited to strikes, if such strikes are reasonably avoidable. A delay caused by a strike or picketing which constitutes an unfair labor practice is not excusable unless the Contractor takes all reasonable and appropriate action to end such a strike or picketing, such as the filing of a charge with the National Labor Relations Board, the use of other available Government procedures, and the use of private boards or organizations for the settlement of disputes.

(End of clause)

3052.222-71	**Strikes or Picketing Affecting Access to a DHS Facility**	**DEC 2003**

If the Contracting Officer notifies the Contractor in writing that a strike or picketing: (a) is directed at the Contractor or subcontractor or any employee of either; and (b) impedes or threatens to impede access by any person to a DHS facility where the site of the work is

located, the Contractor shall take all appropriate action to end such strike or picketing, including, if necessary,, the filing of a charge of unfair labor practice with the National Labor Relations Board or the use of other available judicial or administrative remedies.

(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 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 under this Contract:

Title	Individual Name
Senior Latent Print Examiner/Scientist	To Be Determined at Contract Award

(End of clause)

3052.240-71	**Contractor Employee Access (Deviation CD 25-12)**	**SEP 2025**

(a) *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, 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.

(b) *Information Resources* means information and related resources, such as personnel, equipment, funds, and information technology.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted or subject to other investigations as required. All Contractor employees requiring recurring access to government facilities or access to CUI or information resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to CUI. The Contractor shall access and use CUI only for the purpose of furnishing advice or assistance directly to the Government in support of the Government's activities, and shall not disclose, orally or in writing, CUI for any other purpose to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized to access CUI, the Contractor shall ensure that these persons receive initial and refresher training concerning the protection and

disclosure of the CUI. Initial training shall be completed within 60 days of contract award and refresher training shall be completed every 2 years thereafter.

(f) The Contractor shall include this clause in all subcontracts at any tier where the subcontractor may have access to government facilities, CUI, or information resources.

Alternate I (JUL 2023)

When the contract will require Contractor employees to have access to information resources, add the following paragraphs:

(g) Before receiving access to information resources under this contract, the individual must complete a security briefing; additional training for specific categories of CUI, if identified in the contract; and any nondisclosure agreement furnished by DHS. The Contracting Officer's Representative (COR) will arrange the security briefing and any additional training required for specific categories of CUI.

(h) The Contractor shall have access only to those areas of DHS information resources explicitly stated in this contract or approved by the COR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information resources not expressly authorized by the terms and conditions in this contract, or as approved in writing by the COR, are strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for DHS. It is not a right, a guarantee of access, a condition of the contract, or government-furnished equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management, or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) There must be a compelling reason for using this individual as opposed to a U.S. citizen; and

(2) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall be reported to the Contracting Officer.

(End of clause)

3052.240-72	**Safeguarding of Controlled Unclassified Information (Deviation CD 25-12)**	**SEP 2025**

(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 the 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 Public Law 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 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 Admins 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

names, 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, comprise 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 the 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, comprised, 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 context 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 thread 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. The 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 COS 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/projectscryptographic-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. Receipts 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 with 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 (DEVIATION HSAR CD 25-12) (SEP 2025)

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 created 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, as 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 Contactor 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 form government tools and infrastructure.

(End of clause)

3052.204-73	**Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents (DEVIATION HSAR CD 25-12)**	**SEP 2025**

(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 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 identifiable numbers (PINs).

(3) Other PII that my 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.

(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 the 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 and 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)

	HSAR Information Technology Security Awareness Training	**JUL 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 Rule 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 clause)

Invoicing and Final Payment Instructions (Addendum to 18a of Standard Form (SF) 1449)).

In accordance with FAR 52.212-4(g)(1), invoices shall be submitted either by email or U.S. mail as instructed below in (a) or (b).

(a) USCIS' preferred method for invoice submission is electronically. Electronic invoices shall be submitted in Adobe PDF format with each pdf file containing only one (1) Invoice. The pdf file shall be submitted electronically to USCISInvoice.Consolidation@ice.dhs.gov with each email conforming to a size limit of 500 KB.

(b) If a paper invoice is submitted, mail the invoice to:

USCIS Invoice Consolidation
PO Box 1000
Williston, VT 05495
(802) 288-7600

(c) Direct payment inquiries to I.C.E. Financial Operations, (877) 491-6521.

(End of instruction)

FINAL PAYMENT

As a condition precedent to final payment, a release discharging the government, its officers, agents, and employees of and from all liabilities, obligations, and claims arising out of or under this contract shall be completed. A release of claims will be forwarded to the contractor at the end of each performance period for contractor completion, within thirty (30) days of final invoice submission.

(End of instruction)

Posting of Contract/Order in FOIA Reading Room

Within 30 days of award, the Contractor shall submit a redacted copy of the executed contract/order (including all attachments) suitable for public posting under the provisions of the Freedom of Information Act (FOIA), 5 U.S.C. § 552. The Contractor shall submit both a redacted and unredacted copy of the documents, along with the name of a point of contact and that individual's contact information, to the USCIS FOIA Office via email at err.uscis@uscis.dhs.gov, with a courtesy copy to the USCIS Contracting Officer (CO). With regards to the redacted copy of the executed contract/order, the Contractor will only propose redactions that it, in good faith, believes are exempt from public release pursuant to an applicable FOIA exemption(s). The USCIS FOIA Office will notify the contractor, via the provided point of contact, of any disagreements with the contractor's redactions before public posting of the contractor/order in a public FOIA reading room. Such notice by the USCIS FOIA Office will be consistent with the provisions set forth in 6 C.F.R. § 5.7.

Contractor Performance Assessment Reporting System (CPARS)

The Government intends to record and maintain contractor performance information for this contract in accordance with FAR Subpart 42.15 – Contractor Performance Information. The contractor will need to enroll at www.cpars.gov, so it can participate in this process.

U.S. Citizenship and Immigration Services (USCIS) Personnel Emergency Notification System (PENS) and Contractor Emergency Notification and Accountability Requirements.

1. Government Notification System: USCIS PENS

The USCIS Personnel Emergency Notification System (PENS) is the official USCIS System of record for emergency notifications and personnel accountability and is one of multiple lines of communication utilized during emergency events, both during normal duty hours and non-duty hours. PENS is accessible by USCIS contractor employees issued network accounts with a USCIS email address, as well as other contractor personnel authorized and previsioned PENS accounts by USCIS. PENS is used to push emergency event notifications requiring timely actions and/or responses, such as fires, unexpected weather events, terrorist attacks, cybersecurity breaches, and other emergencies. The current designated application for USCIS's PENS is the Blackberry AtHoc software application.

(a) **Government-owned IT Equipment:** The PENS application will be available on government-owned IT equipment, and contract employees will access it using their USCIS government email account.

(b) Contractor/Employee-owned IT Equipment. Use of PENS on company-owned or employee-owned equipment is optional. Contractor employees with USCIS email addresses may use the Blackberry AtHoc app on personal equipment to receive USCIS emergency notifications by logging in with their USCIS email addresses.

2. Contractor Emergency Notification and Accountability Requirements

(a) Definitions.

(1) Emergency: Any incident beyond routine procedures necessitating urgent action to protect people, property, mission, and infrastructure.

(2) Contractor Employee: Individuals employed by the contractor or its subcontractor(s) performing work or providing services under this contract.

(3) Work Site Code: A unique code provided by USCIS that PENS uses to identify the workplace affiliation of a federal employee or contractor.

(b) Contractor Points of Contact (POC)

(1) Contractors must designate a POC and alternate to receive PENS notification for all contractor employees associated with the Work Site Codes (WSC) where they perform work, including remote personnel physically traveling to a government facility to receive government-furnished equipment (GFE), IT support, or attend meetings. Contractor POCs serve as the primary coordination point of relaying PENS notifications to contractor employees who don't have USCIS email addresses, and for gathering accountability information during emergency events.

(i) Contractor POCs with a USCIS email address serve as first-line Accountability Officers after completing required training. Training can be accessed here.

(ii) Contractor POCs without a USCIS email address receive system access from the PENS team as required.

(2) The contractor must provide the Contracting Officer's Representative (COR) with the identification of all POCs, POC contact information, a list of contractor employees assigned to each POC, and identification of all government facilities where the contractor has personnel assigned (including sites where remote personnel receive USCIS IT support or GFE). Contractors must submit this information using the spreadsheet template found here. This information must be updated in the system and submitted to the COR within 14 calendar days of any change, including employees who have been removed from the contract.

(3) POCs must be subscribed to all applicable WSCs covering their workforce.

(4) A PENS notification account for a primary and alternate contractor POC will be established by USCIS, which may include POCs without USCIS email addresses. POCs will be responsible for collecting accountability information and uploading status into PENS on behalf of contractor employees unable to update PENS.

(c) PENS Maintenance

(1) PENS Profile: Contractors must ensure all contractor employees with USCIS email addresses maintain accurate and current profile information in PENS, including WSC information corresponding to their assigned facility or support location using the Validate User Profile and Subscription knowledge base. Updates must be reflected in PENS profiles within 14 calendar days of any change.

(2) myAccess/ICAM Emergency Contact: If contractor employees choose to update the After Hours and Emergency Center (AHEC) contact information in the myAccess portal (ICAM system), contractors must ensure contractor employees maintain accurate information, updating within 14 calendar days of any change.

(d) Notification and Accountability Requirements

(1) Notification: In the event of an emergency impacting contract performance or personnel safety/security; the contractor must immediately notify the contracting officer and COR. If immediate notification is not possible due to life, safety, or security concerns, notification must occur as soon as conditions allow.

(2) Accountability (responding to PENS notifications): Procedures vary based on employee access to PENS. Contractors must establish internal processes for POCs to push notifications to contractor employees from PENS or alternative means during system outages.

(i) With USCIS Email Accounts: Contractor employees are required to respond directly to all PENS notifications and comply with accountability instructions. During duty hours, report accountability via PENS within 1 hour of an event. For incidents occurring during non-duty hours, report accountability upon signing into the system during the next duty day.

(ii) Without USCIS Email Accounts: Contractor POCs are responsible for emergency notification and accountability reporting for these employees. Contractor employees must respond to

accountability instructions issued by their POC and provide accurate status updates when contacted for accountability. Contractor POCs must make positive contact with assigned contractor employees during Accountability Events to determine their status and then report it to the COR/facility PENS Operator to upload accountability status into PENS. During duty hours, accountability must be reported to the POC within 1 hour of an event and updated within PENS as soon as possible thereafter. For incidents occurring during non-duty hours, accountability should be reported upon signing into the system during the next duty day.

(3) Coordination. Contractor POCs must coordinate with the COR to ensure accurate and timely accountability reporting.

(e) Accountability Exercises

USCIS may conduct periodic emergency notification exercises using PENS. Contractors must participate for employees required to use PENS and provide accountability as addressed above in (f). The Government may conduct up to two facility evacuation/accountability exercises per year.

(f) Cooperation with Government Authorities

Contractors must cooperate fully with Government authorities and emergency responders during emergencies, including providing access to facilities, resources, or personnel as necessary.

(g) Subcontracts

Contractors must flow down these requirements to all subcontractors. Prime contractors retain sole responsibility for communications and reporting between subcontractors and the Government.

(h) Disclaimer of Responsibility

The Government will not be responsible for any outages or disruptions in the functionality of PENS.

(i) Effect of Notifications on Contract Terms

Under no circumstances will a notification pushed from PENS be considered a modification to this contract. To the extent an emergency event affects performance of the contract, it must be addressed with the contracting officer and consideration, if any, for either party must be negotiated and agreed to in writing.

Part III – List of Attachments

Attachment I – Statement of Work, 10 pages

Attachment II – Security Requirements, 6 pages

Part IV – Solicitation Provisions/Instructions/Evaluation

Federal Acquisition Regulation (FAR) Provisions Incorporated by Reference

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 offeror. 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 offeror. Also, the full text of a solicitation provision may be accessed electronically at this address:

https://www.acqusition.gov

(End of provision)

FAR Provisions Incorporated by Reference

52.203-11	**Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions**	**SEP 2024**
52.203-18	**Prohibition on Contracting with Entities that Require Certain Confidentiality Agreements or Statements**	**JAN 2017**
52.204-7	**System for Award Management – Registration (DEVIATION 25-19)**	**NOV 2025**
52.212-1*	**Instruction to Offerors – Commercial Products and Commercial Services (AUG 2025) (DEVIATION 25-21)***	**NOV 2025***
52.212-2*	**Evaluation – Commercial Products and Commercial Services (AUG 2025) (DEVIATION 25-21)**	**NOV 2025***
52.240-90	**Security Prohibitions and Exclusions Representations and Certification (DEVIATION 25-23)**	**NOV 2025**
***See Addendums to these provisions in the "Additional Provisions/Instructions/Evaluation" section below**		

FAR Provisions Incorporated by Full Text

52.252-5	**Authorized Deviations in Provision**	**NOV 2020**

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

(b) The use in this solicitation of any Homeland Security Acquisition Regulation (48 CFR 30) provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of provision)

52.209-7	**Information Regarding Responsibility Matters (NOV 2025) (DEVIATION 25-27)**	**NOV 2025**

(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 a 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 has checked "has" in paragraph (b) of this provision, the offeror represents, by submission of this offeror, 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 offeror 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 reimbursement, restitution, or damages in excess of $100,000.

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

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

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

(End of provision)

52.216-1	**Type of Contract (OCT 2025) (DEVIATION 26-04)**	**NOV 2025**

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

(End of provision)

52.233-2	**Service of Protest**	**SEP 2006**

(a) Protest, as defined in section 33.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), shall be served on the Contracting Officer (addressed as follows) by obtaining written and dated acknowledgement of receipt from:

Gregory Forrest, Contracting Officer
Department of Homeland Security

Citizenship and Immigration Services
Office of Contracting
5900 Capital Gateway Dr.
Camp Springs, MD 20588

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

(End of provision)

HSAR Provisions Incorporated by Full Text

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.

(g) 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 –

(g) 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.

I 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 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 such 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.

I 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

(3) 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 provision)

Additional Provisions/Instructions/Evaluation

Addendum to 52.212-1 – Instructions to Offerors – Commercial Products and Commercial Services

A. The procedures of FAR Part 15 will not be used for this acquisition conducted under FAR Part 12.201-1.

B. The Government intends to award one firm-fixed-price Contract to the responsible offeror whose quote represents the best value to the government. The Government will

perform a comparative evaluation (comparing offers to each other) to select the offeror that provides the best value, considering the evaluation factors below.

Offerors should submit their quotes in two volumes:

- Volume 1, Technical, inclusive of Evaluation Factor 1
- Volume 2, Business, inclusive of Evaluation Factor 2, and any representations/certifications or solicitation/amendment acknowledgments

The following format restrictions apply:

- Volume 1 shall not exceed 5 single-sided pages. In the event a quote exceeds 5 single-sided pages, only the first 5 pages of the quote will be evaluated. Cover pages and contents pages do not count against this page limitation. Fonts utilized shall be no smaller than 10-point font, including in charts/tables/graphs.
- Volume 2 does not have any page limits or format restrictions with regard to font or size. However, offerors must complete and submit the "PRICE PROPOSAL WORKSHEET" table listed below in this clause under Evaluation Factor 2, Price, to submit its total price quote.

Evaluation Factor 1, Technical Approach

The offeror shall describe in detail how it will perform the requirements of Attachment 1, Statement of Work (SOW). Regurgitation of SOW requirements will not be considered, nor will generic statements such as "Contractor will comply."

Evaluation Factor 2, Price

The Offeror shall provide a Firm-Fixed Price (FFP) quote that reflects its proposed solution to the Government's requirement. Offeror shall complete the following table to establish its total quoted price:

PRICE PROPOSAL WORKSHEET		
Base Period (09/30/2026 – 09/29/2027)		
CLIN 0001, Scientific and Program Support Services	Monthly Price: $	Annual Price: $
CLIN 0002, Other Direct Cost: Travel	Reimbursable Travel	Not-to Exceed $18,310.00
CLIN 0003, Expert Witness Testimony	Hourly Rate: $ / Hour	Not-to-Exceed Annual Price for 200 Hours: $
Option Period 1 (09/30/2027 – 09/29/2028)		
CLIN 1001, Expert Witness Testimony	Hourly Rate: $ / Hour	Not-to-Exceed Annual Price for 500 Hours: $
CLIN 1002, Other Direct Costs: Travel	Reimbursable Travel	Not-to-Exceed $48,400.00

CLIN 1003, Quantity Option Additional Scientific and Program Support Services	Monthly Price: $	Annual Price: $
Option Period 2 (09/30/2028 – 09/29/2029)		
CLIN 2001, Expert Witness Testimony	Hourly Rate: $ / Hour	Not-to-Exceed Annual Price for 1200 Hours: $
CLIN 2002, Other Direct Costs: Travel	Reimbursable Travel	Not-to-Exceed $99,300.00
Option Period 3 (09/30/2029 – 09/29/2030)		
CLIN 3001, Expert Witness Testimony	Hourly Rate: $ / Hour	Not-to-Exceed Annual Price for 1200 Hours: $
CLIN 3002, Other Direct Costs: Travel	Reimbursable Travel	Not-to-Exceed $101,800.00
Totals		
	CLIN 0001:	
	CLIN 0002:	$18,310.00
	CLIN 0003:	
	CLIN 1001:	
	CLIN 1002:	$48,400.00
	CLIN 1003:	
	CLIN 2001:	
	CLIN 2002:	$99,300.00
	CLIN 3001:	
	CLIN 3002:	$101,800.00
	Total Quoted Price:	

Quote Due Date

Quotes shall be submitted via e-mail sent directly to the Contract Specialist and Contracting Officer at the following addresses: vanh.phun@uscis.dhs.gov and gregory.e.forrest@uscis.dhs.gov. The Offeror's e-mail subject line shall read: 70SBUR26Q00000188 – Print and Friction Ridge Examinations and Related Services – [Offeror's Contractor Name]. The total size per email shall not exceed 10 megabytes to ensure receipt by the U.S. Government email systems.

Quotes are due no later than August 17th, 2026 at 5:00 PM ET.

Addendum to 52.212-2 – Evaluation – Commercial Products and Commercial Services

A. The Government intends to award one (1) firm-fixed-price Contract resulting from this solicitation to the responsible vendor that represents the best value to the government following a comparative evaluation (comparing offers to each other) of quotations, price and other factors considered.

Evaluation Factor 1 – Technical Approach

The Government will assess the effectiveness of Offeror's approach for successful completion of the requirements of the Statement of Work (Attachment 1).

Evaluation Factor 2 – Price

Price refers to the total quoted price of performing the requirements of the solicitation. The vendor's total quoted price will be evaluated for consistency and arithmetic accuracy, and if any math errors are found the government will, through clarifications, ask the quoting contractor to resolve any math errors. The Government will evaluate the Offeror's total quoted price to determine if the price is fair and reasonable. The Government will evaluate for reasonableness in accordance with one or more price analysis techniques identified in FAR 12.204(a). The Government will evaluate total price inclusive of all options. The Government is not required, but reserves the right, to conduct a price realism analysis if it is deemed necessary within the discretion of the contracting officer.