U.S. Department of Homeland Security
United States Coast Guard

Commanding Officer
United States Coast Guard

2703 Martin Luther King Jr. Ave. SE
Washington, DC 20593-7828
Staff Symbol: CG-HCA-COCO-23
Phone: 571-607-4824
Email: Terry.L.Newton@uscg.mil

June 17, 2026

To: Quoters

Subject: Request for Quote (RFQ) No. 70Z02326QSHIPHULL
Maritime Safety Center Engineering and Technical Support Services

The United States Coast Guard (USCG) Maritime Safety Center (MSC) invites your company to submit a quote in response to the subject RFQ.

All responses to this RFQ shall be submitted electronically by email to the address provided below before the deadline specified in the below instructions.

This acquisition is being conducted pursuant to Federal Acquisition Regulation (FAR) Subpart 12.201-1 Simplified procedures. This acquisition is 100% small business set-aside and is being issued under NAICS 541330 Exception 3 (Marine Engineering and Naval Architecture). The primary place of performance will be designated by the contractor. Subject to space availability and the COR's approval, place of performance may be at the Department of Homeland Security at the U.S. Coast Guard Headquarters, 2703 Martin Luther King Jr. Ave SE, Washington, D.C. 20593-7430.

The Government contemplates award of one (1) time and materials labor-hour contract with fixed hourly rates; however, the Government reserves the right to make no award at all. This RFQ does not commit the Government to pay for the preparation and submission of a Quote. The Government also reserves the right to award without exchanges or communications based upon initial submissions.

The period of performance (POP) includes a base period and one (1) 12-month option period. The estimated period of performance will be from 09/01/2026 to 08/30/2028.

Any Quote that is non-compliant with any requested submission requirements of this RFQ may immediately be removed from further consideration.

The following shows the anticipated CLIN structure:

Period	CLIN	Contract Type	CLIN Description
Base Period	0001	Time and Material Labor Hour (T&MLH)	Professional Engineering and Technical Support Services in accordance with the Performance Work Statement.
Option Period One (1)	0101	Time and Material Labor Hour (T&MLH)	Professional Engineering and Technical Support Services in accordance with the Performance Work Statement.

Submission Instructions

Quoters shall submit their quote directly to the Contracting Officer via email at Terry.L.Newton@uscg.mil. All quotes are due no later than 23:59 (11:59 PM) ET, on 06 July 2026. All questions or requests for clarifications shall be submitted directly to contracting officer Terry.L.Newton@uscg.mil no later than 23:59 (11:59 PM) ET, on 25 June 2026. Please note this RFQ shall not be considered direction to proceed with the subject effort, nor a promise of future direction to proceed. Quoter is solely responsible for quote costs.

A cover sheet (not to exceed one (1) page) shall be included for all submissions. The cover letter shall be included on Volume I and include the quoter's name and address; U.S. Coast Guard solicitation number; Unique Entity Identifier (UEI); CAGE number; quoter's point of contact including their phone number and e-mail address, and the date the quoter's submission expires. Minimum acceptable font size is no smaller than eleven (11) point and no smaller than ten (10) point for tables, charts, or graphs. Page size shall be letter size (8.5" x 11"); tables, charts, or graphs may be legal size, 8.5" x 14".

It is the quoter's responsibility to ensure sufficient time is provided for electronic submissions to be processed through the Government's electronic point-of-entry. The quoter shall acknowledge the solicitation and all amendments thereto.

The quoter shall submit three (3) volumes. Volume I shall contain the quoter's response to Factor 1, Experience and Factor 2, Management Approach. Page limits will be strictly adhered to. Any pages beyond the limit of the entire volume, will not be evaluated. For example, if the page limit to Factor 1 and Factor 2 combined are five (5) pages, and your volume I contains eight (8) pages, the last three (3) pages of Volume I will be removed and will not be evaluated.

Volume II shall contain the quoter's response to Factor 3, Price. Volume III, if required, shall contain any required acknowledgment of amendments (if required), fillable provisions or clauses (if required), or other information as directed by the Government. There is no page limit to Volume III. All terms (price and non-price) shall be valid for a period no less than 120 days from date of solicitation.

- Volume I – Experience and Management Approach
- Volume II – Price
- Volume III – Acknowledgment of Amendments (if required), fillable provisions or clauses (if required), or other information as directed by the Government

Volume I – Experience and Management Approach

Factor 1 Experience

Factor 1 – Experience (two (2) Page Limit)

Quoters shall demonstrate the following:

- Rhinoceros Ship Hull Modeling Experience
  - Provide relevant commercial or academic project(s), where your firm used Rhinoceros for ship hull modeling, including parametric model creation and automation (Python or Grasshopper).
  - Submit at least one sample ship hull model (.3dm format) created by proposed personnel.
- Hull Design and Hydrostatics Analysis
  - Provide your firm's experience developing and analyzing hydrostatics properties of ships as part of hull modeling projects.
  - Provide your firm's experience generating ship models in any form from:
    - 2D drawings
    - Point clouds
    - Other input
- Python Programming for Naval Architecture
  - Provide your firm's Python programming experience and include specific parts of the coding that proposed personnel completed.

Factor 2 Management Approach

Factor 2 – Management Approach (Three (3) Page Limit, resumes and transition plan do not count toward page limit)

Quoters shall demonstrate in their quote the following:

- Approach to effectively manage the administration of this contract to include managing subcontractors (if applicable), managing contractor employees, and responding to government concerns.
- Resumes shall be submitted for key personnel—each resume shall not exceed two (2) pages. In accordance with HSAR Clause 3052.215-70 and PWS Section 3, the following positions are designated as Key Personnel: Project Engineer.

Volume II – Price

Factor 3 Price

Quoters shall complete and submit Attachment A – Price Sheet by filling in their proposed Labor Category, the estimated hours (level of effort), and the hourly rate for that Labor Category.

It is imperative that the contractor's quoted price accurately reflects the price of the Base Period, the price for Option Period One (1) and the total price for a six (6) month extension under 52.217-8.

Failing to follow instructions may have an impact on the Total Evaluated Price (TEP). All quoted prices shall be fully burdened.

The Government will verify the Contractor's TEP in Attachment A – Price Spreadsheet. The TEP will be calculated by adding the proposed total prices for the Base Period, Option Period One (1), and six (6) month Option under FAR 52.217-8. Pricing will be evaluated to determine if the labor categories and labor rates proposed are appropriate for the USCG's requirements. The Government will consider the level of effort and the labor mix proposed to perform the PWS requirements, as well as determine whether the proposed TEP, is reasonable. If your pricing is based on other than the Government's estimate, then the Government will evaluate its rationale. Additionally, the Government will evaluate proposed labor rates (inclusive of any applicable discounts) for reasonableness. Quotes containing labor rates determined to be unreasonable may result in the Quote being determined non-responsive.

For the purposes of the award of this Order, the Government intends to evaluate the Option to Extend Services in accordance with Federal Acquisition Regulation (FAR) clause 52.217-8 as follows:

To account for the option periods possible under 52.217-8 (maximum of six months), Options to Extend Services, the Government will evaluate the option to extend services by adding six months of the Quoter's final option period price to the Quoter's total price. This amount will be the Total Evaluated Price. The Government may choose to exercise the Option to Extend Services at the end of any performance period (base or option period). Prices for the Base and Option Periods, including the 6-month option available under FAR 52.217-8, will be evaluated to ensure that they are fair and reasonable for performance of the requirements established in the solicitation and as proposed in the technical submission. The price for the effort associated with FAR 52.217-8 will not be included in the total awarded value at order award. If, at the end of the period of performance (the end of the Base period or any Option Period) and within the time period established in the clause, the Government chooses to exercise this option, the pricing will be pursuant to the rates specified in the order for the preceding performance period.

Cells have <u>not</u> been locked and some cells contain formulas. Only cells in gray may be filled in by the quoter.

The quoter shall populate their solution's Labor Categories (C5 and C7), and the corresponding Hourly Rate for that Labor Category (C5 and C7). The quoter shall complete the estimated number of hours for each Labor Category (D5 and D7).

Through formulas, the pricing sheet provides the Base Price + Option Period One, and the Total Evaluated Price (which includes the Option Period for up to Six Months (FAR R 52.217-8). These cells auto-populate based on quoter inputs and shall not be manipulated.

The Government requests that the quoter consider discounting to the maximum extent possible.

Evaluation Criteria

Basis of Award

The Government intends to award one order resulting from this solicitation to the responsible Quoter whose offer conforming to the solicitation represents the best value (as defined in FAR 2.101) to the Government utilizing a trade-off evaluation process among price and non-price factors. Best value trade-off will be based on the following evaluation factors: Factor 1, Experience; Factor 2, Management Approach and Factor 3, Price.

Experience is more important than Management Approach, and when combined are significantly more important than Price.

Factor 1 Experience

The Government will assess its level of confidence for each Quoter based on the Quoter's approach to:

- Rhinoceros Ship Hull Modeling Experience
- The number of projects completed using Rhinceros for ship hull modeling.
- Complexity and scale of projects (ex., size of vessels, level of detail.
- Inclusion of parametric model creation and automation techniques (Python or Grasshopper).
- Use of Python computer programming.

- Hull Design and Hydrostatics Analysis
- Specific examples of hydrostatics properties analyzed.
- Tools and methodologies used for hydrostatic analysis.
- Integration of hydrostatic analysis within overall hull modeling projects.

- Python Programming for Naval Architecture
- Number and complexity of Python scripting projects completed for naval architecture.
- Specific applications of Python in ship hull modeling or hydrostatic analysis.
- Clarity and functionality of provided code snippets, including comments and documentation.

Factor 2 Management Approach

The Government will assess its level of confidence for each Quoter based on the Quoter's experience with:

- Effectively manage the administration of this contract to including the management of subcontractors (if applicable), management of their employees, and responding to government concerns.
- Evaluate the quality and applicability of the products submitted to the Government.
- The resume(s) of key personnel to ensure they meet the qualifications listed in Section 3 of the PWS.

Factor 3 Price

The Government will evaluate quotes to verify the accuracy of the quoter's Total Evaluated Price (TEP) provided in Attachment A and will determine whether their proposed TEP is fair and reasonable. The TEP will be calculated by adding together the proposed total prices of the base period and all option periods. Adequate price competition is anticipated to support a determination of a fair and reasonable price.

Except when it is determined in accordance with FAR 17.206(b) not to be in the Government's best interests, the Government will evaluate quotes for award purposes by adding the total price for all options to the total price for the basic requirement to determine the total evaluated price. This includes options under FAR clause 52.217-8 (Option to Extend Services), which applies to this solicitation. Evaluation of options will not obligate the Government to exercise the option(s).

The Government will evaluate quotes for award purposes by adding the total price for all options to the total price for the basic requirement. To account for the option periods possible under 52.217-8 (maximum of six (6) months / Option to Extend Services), the Government will evaluate the option to extend services by adding six (6) months of the quoter's final option period price to the quoter's total price. This amount will be the total evaluated price. The Government may choose to exercise the Option to Extend Services, in total or incrementally, at the end of any performance period (base or option periods). Prices for the base and option periods, including the 6-month option available under FAR 52.217-8, will be evaluated to ensure that they are fair and reasonable for performance of the requirements established in the solicitation and as quoted in the technical submission. The price for the effort associated with FAR 52.217-8 will not be included in the total awarded value at contract award. If, at the end of the contract's/order's period of performance (the end of the base period or any option period) and within the time period established in the clause, the Government chooses to exercise this option, the pricing will be pursuant to the rates specified in the contract for the preceding performance period.

Rating Scheme

The Government will assess its level of confidence for the non-price evaluation Factor 1, Experience and Factor 2, Management Approach.

Rating	Rating Definitions
High Confidence	The Government has *high confidence* that the quoter understands the requirement, quotes a sound approach, and will be successful in performing the contract with *little* or no Government intervention.
Some Confidence	The Government has *some confidence* that the quoter understands the requirement, quotes a sound approach, and will be successful in performing the contract with *some* Government intervention.
Low Confidence	The Government has *low confidence* that the quoter understands the requirement, quotes a sound approach, and will be successful in performing the contact *even with* Government intervention.

The Supplemental Terms and Conditions are below.

Thank you for your support of the United States Coast Guard, and for your consideration of submitting a response to this RFP.

Sincerely,

NEWTON.TERRY.LYNN.1374663450 Digitally signed by NEWTON.TERRY.LYNN.1374663450 Date: 2026.06.17 08:44:20 -04'00'

Terry Newton
Contracting Officer/Contracts Specialist

Attachments:
Attachment I: PWS
Attachment A: Price Input

Supplemental Terms and Conditions

Clauses

Clauses Incorporated by Reference			
Source	Clause	Clause Name	Date
FAR	52.209-10	Prohibition on Contracting with Inverted Domestic Corporations	NOV 2015
FAR	52.212-4	Contract Terms and Conditions—Commercial Products and Commercial Services	NOV 2023
FAR	52.212-4	Contract Terms and Conditions-Commercial Products and Commercial Services-Alternate I	NOV 2021
FAR	52.222-50	Combating trafficking in Persons	OCT 2025
FAR	52.232-40	Providing Accelerated Payments to Small Business Subcontractors	MAR 2023
FAR	52.246-3	Changes-Time-and Materials or Labor-Hours	SEPT 2000

Invoicing Instruction Addenda 52.212-4, Contract Terms and Conditions – Commercial Products and Services

Electronic Submission of Payment Requests (FSMS Awards)

(a) Definitions. As used in these instructions -
(1) "Payment request" means a bill, voucher, invoice, or request for contract financing payment with associated supporting documentation. The payment request must: comply with the requirements identified in FAR 32.905(b), "Content of Invoices" and the applicable Payment clause included in this contract. In addition, discount offerings and small business status if available must be stated. If travel was allowable and approved, components in accordance with FAR 31.205-46 must be provided.

(b) Except as provided in paragraph (c) of this clause, the contractor must submit payment requests electronically using the Invoice Processing Platform (IPP). Information regarding IPP, including IPP Customer Support contact information, is available at www.ipp.gov or any successor site.

(c) The contractor may submit payment requests using a method other than IPP only when the contracting officer authorizes alternate procedures in writing in accordance with Coast Guard procedures.

(d) If alternate payment procedures are authorized, the contractor must include a copy of the contracting officer's written authorization with each payment request.

(e) IPP enrollment information is at https://www.uscg.mil/fincen/IPP/.

(f) Receiving Official: Contracting Officer's Representative

Invoice Approver Official: Contracting Officer's Representative

Mission Partner Identity, Credential and Access Management (MP ICAM)

(a) "Contractor employee" means an employee of a firm, or an individual, under contract or subcontract to the Coast Guard to provide services who also requires one or more of the following:

(1) Physical access to multiple Coast Guard facilities or multiple federally controlled facilities on behalf of the Coast Guard on a recurring basis (a minimum of two (2) times per week and/or eight (8) times per month) for a period of six (6) months or more.

(2) Remote access, via logon, to Coast Guard network using Coast Guard-approved remote access procedures.

(3) Both physical access to Coast Guard facility and logical access, via logon, to Coast Guard networks on-site or remotely. Access to the Coast Guard network must require the use of a computer with government-controlled configuration or use of Coast Guard-approved remote access procedure in accordance with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide.

(b) Homeland Security Presidential Directive (HSPD)-12 mandates a federal standard for secure and reliable forms of identification for federal employees and contractor employees. The Common Access Card (CAC) is a personal identification card for the Department of Defense (DoD)/Uniformed Services and complies with HSPD-12. The Coast Guard has instituted the CAC as its HSPD-12 compliant personal identification card for contractor and subcontractor employees who are required to access a Coast Guard, DoD, or other federally-controlled computer information system and/or facility, or need public key infrastructure (PKI) authentication to perform their contractual duties. The Mission Partner Identity, Credential and Access Management (MP ICAM) (or successor system thereto) is the automated application process for obtaining a CAC.

(c) Contractor and subcontractor employees working pursuant to this contract who are required to access a Coast Guard, DoD, or other federally-controlled computer information system and/or facility, or need PKI authentication to perform their contractual duties must use MP ICAM (or successor system thereto) to obtain a CAC.

(d) The COR or Alternate COR (ACOR) is the MP ICAM Mission Partner Affiliation Sponsor (MPAS) (or successor system corresponding role thereto) and initiates contractor accounts in the MP ICAM (or successor system thereto), approving, returning, or rejecting CAC applications (as applicable); re-verifying assigned contractors every six months; revoking contractor and employee eligibility for a CAC.

(e) The MPAS ensures that contractor personnel satisfy the security requirements for CAC issuance prior to creating the CAC application in MP ICAM (or successor system thereto). Current investigative requirements must be verified according to Commandant Instruction 5500.18. The initial CAC issuance requires a favorably adjudicated Tier 1 investigation (equivalent or higher) or a Tier 1 background investigation (BI) (equivalent or higher) package that has been successfully scheduled with the investigative service provider (ISP) and

an FBI fingerprint check with favorable results. The MPAS and Sponsor (or successor system corresponding role) or other appropriate federal government representative must coordinate with the unit BI Verifier (Command Security Officer / Mission Partner Affiliation Sponsor Manager) or the U.S. Coast Guard Security (SECCEN) to confirm the appropriate investigation has been favorably adjudicated or scheduled at the ISP with favorable FBI fingerprint results.

(f) The COR or contracting officer (KO) provides such forms to, or requests such information from, contractor employees that may be necessary for obtaining a CAC via the MP ICAM (or successor system thereto). The Contractor submits completed forms and information as directed by the COR or KO. Contractors are responsible for the accuracy and completeness of the information submitted and for any liability resulting from the government's reliance on inaccurate or incomplete information.

(g) Contractor employees who are declined via the MP ICAM (or successor system thereto) are ineligible to perform work under this contract.

(h) When an employee with a CAC is no longer performing work under this contract, the employee must return the CAC to the COR/MPAS (or successor system corresponding role thereto) or KO on the same day the employee stops working.

(i) The contractor must insert this requirement in all subcontracts when a subcontractor's employee is required to access a Coast Guard, DoD, or other federally-controlled computer information system and/or facility, or need PKI authentication to perform contractual duties. (h) When an employee with a CAC is no longer performing work under this contract, the employee must return the CAC to the COR/MPAS (or successor system corresponding role thereto) or KO on the same day the employee stops working.

(End of Clause)

FAR 52.203-17 Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights (APR 2024) (DHS-USCG DEVIATION 14-01, Revision 1).

(a) This contract and employees working on this contract will be subject to the whistleblower rights and remedies established at 10 U.S.C. 4701 and Homeland Security Acquisition Regulation (HSAR) 3.900 (DEVIATION) through 3.905 (DEVIATION).

(b) The Contractor shall inform its employees in writing, in the predominant language of the workforce, of employee whistleblower rights and protections under 10 U.S.C. 4701, as described in HSAR 3.900 (DEVIATION) through 3.905 (DEVIATION).

(c) The Contractor shall insert the substance of this clause, including this paragraph (c), in all subcontracts.

(End of clause)

FAR 52.217-8 Option to Extend Services (Nov 1999).

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within **15** days.

(End of clause)

FAR 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 **15** days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend **at** least **30** days before the contract expires. The preliminary notice does not commit the Government to an extension.

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 36 months.

(End of clause)

FAR 52.217-7 Option for Increased Quantity-Separately Priced Line Item (JULY 2024) (DEVIATION 2024-05)

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 30 days. For services, this shall be no less than 10 calendar days before services commence. For supplies, delivery of added items shall continue at the same rate that like items are called for under the contract, unless the parties otherwise agree. Performance of added services shall comply with the requirements identified in the Schedule.

(End of clause)

FAR 52.224-3 Privacy Training – Alternate I (DEVIATION).

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

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

(1) Have access to a system of records;

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

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

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

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

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

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

(1) Have access to a system of records;

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

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

(End of clause)

FAR 52.232-18 Availability of Funds (APR 1984).

Pursuant to FAR clause 52.232-18, funds are not presently available for this contract. The Government's obligation under this contract is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are made available to the Contracting Officer for this contract and until the Contractor receives notice of such availability, to be confirmed in writing by the Contracting Officer.

(End of clause)

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

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

American Security Drone Act-covered foreign entity means an entity included on a list that the Federal Acquisition Security Council (FASC) develops and maintains and publishes in the

System for Award Management (SAM) at https://www.sam.gov (section 1822 of Pub. L. 118-31, 41 U.S.C. 3901 note prec.).

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

Covered application means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited. 39

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

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

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

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

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

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

Covered telecommunications equipment or services means—

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

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

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

Critical technology means—

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

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

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

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

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

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

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

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

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

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

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

(1) 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.
(2) The Director of National Intelligence (DNI) may issue FASCSA orders that apply to the intelligence community and sensitive compartmented information systems, to the extent not covered by paragraph (2) of this definition. This type of FASCSA order may be referred to as a DNI FASCSA order.

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

(1) Means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management,

movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use—

(i) Of that equipment; or

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

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

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

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

(1) The Office of the Director of National Intelligence;
(2) The Central Intelligence Agency;

(3) The National Security Agency;

(4) The Defense Intelligence Agency;

(5) The National Geospatial-Intelligence Agency;

(6) The National Reconnaissance Office;

(7) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs;
(8) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy;
(9) The Bureau of Intelligence and Research of the Department of State;
(10) The Office of Intelligence and Analysis of the Department of the Treasury;
(11) The Office of Intelligence and Analysis of the Department of Homeland Security; or

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

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately

delivered (e.g., connecting a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

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

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

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

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

Kaspersky Lab-covered entity means—

(1) Kaspersky Lab;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(1) A covered application on any information technology owned or managed by the Government, or on any information technology used or provided by the Contractor under this contract, including equipment provided by the Contractor's employees (section 102 of Division R of the Consolidated Appropriations Act, 2023 (Pub. L. 117-328));
(2) A Kaspersky Lab-covered article (Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91));
(3) Covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system (paragraphs (a)(1)(A) of section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232)). This does not prohibit contractors from providing—

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

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

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

(1) Prohibition. The Contractor is prohibited from—

(i) Delivering any FASC-prohibited unmanned aircraft system, which includes unmanned aircraft (i.e., drones) and associated elements (sections 1823 and 1826 of American Security Drone Act of 2023, within the National Defense

Authorization Act for Fiscal Year 2024, Pub. L. 118-31, Div. A, Title XVIII, Subtitle B, 41 U.S.C. 3901 note prec.);

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

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

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

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

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

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

(i) Unless an applicable waiver has been issued by the Government, the Contractor cannot use any equipment, systems, or services that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system (paragraph (a)(1)(B) of section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232)).

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

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

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

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

(i) Except as authorized by the Office of Foreign Assets Control (OFAC) in the Department of the Treasury, the Contractor shall not acquire, for use in the performance of this contract, any supplies or services if any proclamation, Executive order, or statute administered by OFAC, or if OFAC's implementing

regulations at 31 CFR chapter V, would prohibit such a transaction by a person subject to the jurisdiction of the United States.

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

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

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

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

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

(4) *Iran prohibitions*.

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

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

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

(iv) Unless an exception applies or the Government grants a waiver, contractors are prohibited from knowingly engaging in any significant transaction (i.e., over $10,000) with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked according to the International Emergency Economic Powers Act (section 6(b)(1)(B) of Iran Sanctions Act (50 U.S.C. 1701 note)).

(e) *Governmentwide exclusion and removal orders*.

(1) Unless the Government has issued an applicable waiver, contractors shall not provide or use as part of the performance of the contract any covered article, or any products or services produced or provided by a source, if the covered article or the source is prohibited by an applicable FASCSA order as follows:
   (i) For solicitations and contracts awarded by a Department of Defense contracting office, DoD FASCSA orders apply.
   (ii) For all other solicitations and contracts, DHS FASCSA orders apply.
(2) The Contractor shall search for the phrase "FASCSA order" in the System for Award Management (SAM) at https://www.sam.gov to locate applicable FASCSA orders.
(3) The Government may identify in the solicitation other FASCSA orders that are not in SAM, which are effective and apply to the solicitation and resulting contract.

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

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

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

(h) *General report*.

(1) If the Contractor identifies or is notified by any source, (including a subcontractor at any tier), that any product or service provided or used (or to be provided or used) during contract performance does not comply with any prohibition in this clause, then the Contractor shall report the following information, or as much information is known, in writing to the contracting office as identified in paragraph (h)(2) within 72 hours:

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

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

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

   (iv) The entity that produced the product or service (include entity name, unique entity identifier, Contractor and Government Entity (CAGE) code,

facilities responsible for design, fabrication, assembly, packaging, and test of the product, and whether the entity was the OEM or a distributor (provide manufacturer codes and distributor codes used for the product));

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

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

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

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

(A) Brand;

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

(C) Item description, as applicable.

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

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

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

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

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

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

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

(i) *New FASCSA orders report*.

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

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

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

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

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

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

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

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

(End of clause)

FAR 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 _____ *[insert regulation name]* (48 CFR) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of clause)

HSAR 3052.204-71 Contractor Employee Access. (JUL 2023).

(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 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 II (JUL 2023)

When the Department has determined contract employee access to controlled unclassified information or Government facilities must be limited to U.S. citizens and lawful permanent residents, but the contract will not require access to information resources, add the following paragraphs:

(g) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee.

(h) Contractors shall identify in their Quotes, 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 also be reported to the Contracting Officer.

(End of clause)

Alternate II (JUL 2023)

When the Department has determined contract employee access to controlled unclassified information or Government facilities must be limited to U.S. citizens and lawful permanent residents, but the contract will not require access to information resources, add the following paragraphs:

(g) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee.

(h) Contractors shall identify in their Quotes, 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 also be reported to the Contracting Officer.

(End of clause)

3052.204-72 Safeguarding of Controlled Unclassified Information (JUL 2023).

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

Adequate Security means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls. *Controlled Unclassified Information (CUI)* is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

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

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through 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 Program Manager Designee;

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

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

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

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

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

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

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

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

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

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

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

any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

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

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

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

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

Federal information means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

Federal information system means an information system used or operated by an agency or by a Contractor of an agency or by another organization on behalf of an agency.

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

Incident means an occurrence that—

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

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

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

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

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

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

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

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

(b) *Handling of Controlled Unclassified Information.*

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

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

(3) The Contractor shall not maintain SPII in its invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions. It is acceptable to maintain in these systems the names, titles, and contact information for the Contracting Officer's Representative (COR) or other government personnel associated with the administration of the contract, as needed.

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

(c) *Incident Reporting Requirements.*

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

report is made by phone, or the email address for the Contracting Officer or COR is not immediately available, the Contractor shall contact the Contracting Officer and COR immediately after reporting to the Component or DHS Enterprise SOC.

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

(3) CUI transmitted via email shall be protected by encryption or transmitted within secure communications systems. CUI shall be transmitted using a *FIPS 140–2/140–3 Security Requirements for Cryptographic Modules* validated cryptographic module identified on https://csrc.nist.gov/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. Recipients of CUI information will comply with any email restrictions imposed by the originator.

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

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

(i) Unique Entity Identifier (UEI);

(ii) Contract numbers affected unless all contracts by the company are affected;

(iii) Facility CAGE code if the location of the event is different than the prime Contractor location;

(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, and email);

(v) Contracting Officer POC (address, telephone, and email);

(vi) Contract clearance level;

(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;

(viii) Government programs, platforms, or systems involved;

(ix) Location(s) of incident;

(x) Date and time the incident was discovered;

(xi) Server names where CUI resided at the time of the incident, both at the Contractor and subcontractor level;

(xii) Description of the government PII or SPII contained within the system; and

(xiii) Any additional information relevant to the incident.

(d) *Incident Response Requirements.*

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

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

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

(i) Inspections;

(ii) Investigations;

(iii) Forensic reviews;

(iv) Data analyses and processing; and

(v) Revocation of the Authority to Operate (ATO), if applicable.

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

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

(e) *Certificate of Sanitization of Government and Government-Activity-Related Files and Information.* Upon the conclusion of the contract by expiration, termination, cancellation, or as otherwise indicated in the contract, the Contractor shall return all CUI to DHS and/or destroy it physically and/or logically as identified in the contract unless the contract states that return and/or destruction of CUI is not required. Destruction shall conform to the guidelines for media sanitization contained in NIST SP 800–88, *Guidelines for Media Sanitization.* The Contractor shall certify and confirm the sanitization of all government and government-activity related files and information. The Contractor shall submit the certification to the COR and Contracting Officer following the template provided in NIST SP 800–88, *Guidelines for Media Sanitization,* Appendix G.

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

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

Alternate I (JUL 2023)

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

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

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

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

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the Contractor shall renew the ATO every 3 years. The Contractor is required to update its SA package as part of the ATO renewal process for review and verification of security controls. Review and verification of security controls is independent of the system production date and may include onsite visits that

involve physical or logical inspection of the Contractor environment to ensure controls are in place. The updated SA package shall be submitted for review and approval by the Component or Headquarters CIO, or designee, at least 90 days before the ATO expiration date. The Contractor shall update its SA package by one of the following methods:

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

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

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

(4) *Federal Reporting and Continuous Monitoring Requirements.* Contractors operating information systems on behalf of the Government shall comply with Federal reporting and information system continuous monitoring requirements. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2015 DHS Information Security Performance Plan, or successor publication, accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors. The plan is updated on an annual basis. Annual, quarterly, and monthly data collection will be coordinated by the Government. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for information systems. The Contractor shall provide the COR with requested information within 3 business days of receipt of the request. Unless otherwise specified in the contract, monthly continuous monitoring data shall be stored at the Contractor's location for a period not less than 1 year from the date the data are created. The Government may elect to perform information system continuous monitoring and IT security scanning of information systems from government tools and infrastructure.

(End of clause)

HSAR 3052.215-70 Key Personnel or Facilities (DEC 2003).

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.

(b) Before removing or replacing any of the specified individuals or facilities, the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The

Contractor shall not remove or replace personnel or facilities until the Contracting Officer approves the change.

The Key Personnel or Facilities under this Purchase Order:

- **Project Engineer**

(End of clause)

Notice IAW FAR Class Deviation 25-01 – E.O. 14173 & 14168

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

Provisions

Provisions Incorporated by Reference			
Source	Provision	Provision Name	Date
FAR	52.203-11	Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions*	
FAR	52.203-18	Prohibition on Contracting with Entities that require Certain Internal Confidentiality Agreements of Statements – Representation*	JAN 2017
FAR	52-204-7	System for Award Management *	NOV 2024
FAR	52.209-11	Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law	FEB 2016
FAR	52.212-2	Evaluation of Commercial Products and Commercial Services	
FAR	52.216-31	T&M LH Quote Requirements-Commercial Acquisition	NOV 2021
HSAR	3052.223-90	Accident and Fire Reporting	DEC 2003

FAR 52.233-2 Service of Protest (Sept 2006)

(a) Protests, as defined in section 33.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), shall be served on the Contracting Officer (addressed as follows) by obtaining written and dated acknowledgment of receipt from emailing the Contracting Officer at Terry.L.Newton@uscg.mil and the protest mailbox at protests@uscg.mil.

(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)

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

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

Backhaul, covered article, covered telecommunications equipment or services, critical technology, FASCSA order, Intelligence community, interconnection arrangements, national security system, roaming, sensitive compartmented information, sensitive compartmented information system, source, and substantial or essential component have the meanings provided in the clause 52.240-91, Security Prohibitions and Exclusions.
Business operations means engaging in commerce in any form, including by acquiring, developing, maintaining, owning, selling, possessing, leasing, or operating equipment, facilities, personnel, products, services, personal property, real property, or any other apparatus of business or commerce.
Marginalized populations of Sudan means—

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

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

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

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

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

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

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

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

(6) Have been voluntarily suspended.

Sensitive technology—

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

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

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

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

(b) *Procedures*.

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

(2) *FASCSA Orders*.

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

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

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

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

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

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

(d) *FASCSA Representation*. By submission of this offer, the offeror represents that it has conducted a reasonable inquiry, and that the offeror does not propose to provide or use in response to this solicitation any covered article, or any products or services produced or provided by a source, if the covered article or the source is prohibited by an applicable FASCSA order in effect on the date the solicitation was issued, except as waived by the solicitation, or as disclosed in paragraph (g). A reasonable inquiry will look at any information in the offeror's possession but does not need to include an internal or third-party audit.

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

(f) *Iran Representation and Certifications*.

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

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

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

(iii) Certifies that the offeror, and any person owned or controlled by the offeror, does not knowingly engage in any transaction that exceeds $10,000 with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (see OFAC's Specially Designated Nationals and Blocked Persons List at https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx)

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

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

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

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

(g) *Disclosure*.

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

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

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

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

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

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

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

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

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

(A) Brand;

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

(C) Item description, as applicable.

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

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

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

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

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

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

(End of Provision)