Part 40 - Information Security and Supply Chain Security

40.000 Scope of part.

(a) This part addresses broad security requirements that apply to acquisitions of products and services. It outlines policies and procedures for managing information security and supply chain security when acquiring products and services that include, but are not limited to, information and communications technology (ICT).

(b) See parts 24 and 46 for more policies and procedures related to managing information security and supply chain security.

(c) Information and supply chain policies and procedures that are unrelated to security are covered in other parts of the FAR (*e.g.*, part 22 for labor and human trafficking risks and part 23 for climate-related risks).

40.001 Definition.

As used in this part:

Supply chain risk, as defined in 41 U.S.C. 4713(k), means the risk that any person may sabotage, maliciously introduce unwanted functionality, extract data, or otherwise manipulate the design, integrity, manufacturing, production, distribution, installation, operation, maintenance, disposition, or retirement of covered articles so as to surveil, deny, disrupt, or otherwise manipulate the function, use, or operation of the covered articles or information stored or transmitted on the covered articles.

Subpart 40.1 - Processing Supply Chain Risk Information

40.101 Definition.

As used in this subpart:

Supply chain risk information includes, but is not limited to, information that describes or identifies:

(1) Functionality and features of covered articles, including access to data and information

system privileges;

(2) The user environment where a covered article is used or installed;

(3) The ability of a source to produce and deliver covered articles as expected;

(4) Foreign control of, or influence over, a source or covered article (e.g., foreign ownership, personal and professional ties between a source and any foreign entity, legal regime of any foreign country in which a source is headquartered or conducts operations);

(5) Implications to government mission(s) or assets, national security, homeland security, or critical functions associated with use of a covered source or covered article;

(6) Vulnerability of Federal systems, programs, or facilities;

(7) Market alternatives to the covered source;

(8) Potential impact or harm caused by the possible loss, damage, or compromise of a product, material, or service to an organization's operations or mission; and

(9) Likelihood of a potential impact or harm, or the possible exploitation of a system;

(10) Security, authenticity, and integrity of covered articles and their supply and compilation chains;

(11) Capacity to mitigate risks identified;

(12) Factors that may reflect upon the reliability of other supply chain risk information; and

(13) Any other considerations that would factor into analyzing the security, integrity, resilience, quality, trustworthiness, or authenticity of covered articles or sources.

40.102 Sharing supply chain risk information.

Executive agencies must share relevant supply chain risk information with the Federal Acquisition Security Council if the executive agency determines there is a reasonable basis to conclude a substantial supply chain risk associated with a source or covered article exists (see 41 CFR 201-1.201).

Subpart 40.2 - Security Prohibitions and Exclusions

40.201 Definitions.

As used in this subpart:

American Security Drone Act-covered foreign entity means an entity included on a list

developed and maintained by the Federal Acquisition Security Council (FASC) and published 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).

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.

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

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

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

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

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

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

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

Covered telecommunications equipment or services means_

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

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

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

such equipment; or

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

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

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

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

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

Federal Acquisition Security Council (FASC) means the Council established under 41 U.S.C. 1322(a).

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 DoD 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.

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.

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.

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.

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.

*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)).

40.202 Prohibitions.

Agencies are prohibited from contracting, including renewing or extending contracts, with contractors that operate, provide, and/or use certain products or services that violate any of the following prohibitions (see the clause at 52.240-91 for details regarding the scope of each prohibition and whether there are any exceptions, exemptions, or waiver possibilities):

(a)*TikTok/ByteDance.* Covered Application (Section 102 of Division R of the Consolidated Appropriations Act, 2023 (Pub. L. 117-328));

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

(c)*Drones.* Unmanned Aircraft Systems Manufactured or Assembled by American Security Drone Act_Covered Foreign Entities (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.));

(d)*Telecommunications and Video Surveillance Equipment*. (Paragraphs (a)(1)(A) and (a)(1)(B) of section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232));

(e)*Governmentwide Exclusion Orders*. FASCSA orders (sections 1823 and 1826 of Pub. L. 118-31, 41 U.S.C. 3901 note prec.);

(f)*Office of Foreign Assets Control (OFAC) Restrictions*. OFAC Restrictions (International Emergency Economic Powers Act (IEEPA) (50 U.S.C. 1701 et seq.));

(g)*Sudan Prohibition*. Accountability and Divestment Act of 2007 (Pub. L. 110-174); and

(h)*Iran Prohibitions*. Section 6(b)(1)(A) of Iran Sanctions Act (50 U.S.C. 1701 note) and section 6(b)(1)(B) of Iran Sanctions Act (50 U.S.C. 1701 note).

40.203 General Procedures.

40.203-1 Assessment of proposals.

Except where an exemption, exception, or waiver applies, the contracting officer should work with the program office or requiring activity to review proposals if needed to ensure they are not proposing delivery of a product or service in violation of the prohibitions in FAR 40.202, such as a FASC-prohibited unmanned aircraft system (drone).

40.203-2 Waivers.

If the offeror submits a disclosure according to FAR 52.240-90, the contracting officer must follow agency procedures to determine if an exception or exemption applies with any

prohibition, or if a waiver may be applicable in accordance with 40.203-3.

40.203-3 Waivers.

(a) An acquisition may be either fully or partially covered by a waiver. Partial waiver coverage occurs when only portions of the products or services being procured or provided by a source are covered by an applicable waiver. If the requiring activity notifies the contracting officer that the acquisition is partially covered by an approved individual waiver or class waiver, then the contracting officer must work with the program office or requiring activity to identify in the solicitation, request for quotation, or order the products or services that are subject to the waiver.

(b) The contracting officer, in accordance with agency procedures, must decide whether to pursue a waiver or to make award to an offeror that does not require a waiver. If a full or partial waiver is being pursued, then the contracting officer may not make an award until written approval is obtained that the waiver has been granted.

40.203-4 Reporting requirements.

If the offeror submits a disclosure according to FAR 52.240-91, the contracting officer must follow agency procedures to determine if an exception or exemption applies with any prohibition, or if a waiver may be applicable in accordance with 40.203-3.

40.204 Specific Procedures.

40.204-1 Procedures on FASCSA orders.

(a)*Identifying applicable FASCSA orders*. Whether FASCSA orders apply to a particular acquisition depends on the contracting office's agency, the scope of the FASCSA order, the funding, and whether the requirement involves certain types of information systems (see the definition of _FASCSA order_ at 40.201). The contracting officer must coordinate with the program office or requiring activity to identify the FASCSA order(s) that apply to the acquisition as follows:

(1) Unless the program office or requiring activity instructs the contracting officer otherwise, FASCSA orders apply as follows:

(i) Contracts awarded by civilian agencies will be subject to DHS FASCSA orders.

(ii) Contracts awarded by DoD will be subject to DoD FASCSA orders. See paragraph (e)(1) of 52.240-91, Security Prohibitions and Exclusions.

(2) For acquisitions where the program office or the requiring activity instructs the contracting officer to select specific types of FASCSA orders, the contracting officer must select _yes_ or _no_ for each applicable type of FASCSA order. See paragraph (e)(1) of 52.240-91, Security Prohibitions and Exclusions, with its Alternate I.

(b)Federal Supply Schedules, Governmentwide acquisition contracts, and multi-agency contracts specific procedures.

(1) Applying FASCSA orders. An agency awarding this type of contract must apply FASCSA orders to the basic contract award. Ordering activity contracting officers may use this contract vehicle without taking further steps to identify applicable FASCSA orders in the order. The contracting officer awarding the basic contract would select _yes_ for all FASCSA orders (i.e., _DHS FASCSA Order_ _DoD FASCSA Order_ and _DNI FASCSA Order_) (see paragraph (e)(1) of 52.240-91, Security Prohibitions and Exclusions, with its Alternate I). If the contracting officer becomes aware of a newly issued applicable FASCSA order, then the agency awarding the basic contract must modify the basic contract to remove any covered article, or any products or services produced or provided by a source, prohibited by the newly issued FASCSA order.

(2) Interagency acquisitions. For an interagency acquisition (see subpart 17.5) where the funding agency differs from the awarding agency, the funding agency must determine the applicable FASCSA orders.

(c)*Updating the solicitation or contract for new FASCSA orders*. The contracting officer must update a solicitation or contract if the program office or requiring activity determines it needs to:

(1) Amend the solicitation to include FASCSA orders in effect after the date the solicitation was issued but before contract award; or

(2) Modify the contract to include FASCSA orders issued after the date of contract award.

(i) Any such modification should take place within a reasonable amount of time, but no later than 6 months from the program office or requiring activity's determination.

(ii) If the contract is not modified within the time specified in paragraph (c)(2)(i) of this section, then the contract file must be documented giving the reason why the contract could not be modified within this timeframe.

(d)*Agency specific procedures*. The contracting officer must follow agency procedures for implementing FASCSA orders not identified in SAM.

(e)Waivers.

(1) An executive agency required to comply with a FASCSA order may submit a request that the order or some of its provisions not apply to_

(i) The agency;

(ii) Specific actions of the agency or a specific class of acquisitions;

(iii) Actions of the agency for a period of time before compliance with the order is

practicable; or

(iv) Other activities, as appropriate, that the requesting agency identifies.

(2) A request for waiver must be submitted by the executive agency in writing to the official that issued the order, unless other instructions for submission are provided by the applicable FASCSA order.

(3) The request for waiver must provide the following information for the issuing official to review and evaluate the request, including_

(i) Identification of the applicable FASCSA order;

(ii) A description of the exception sought, including, if limited to only a portion of the order, a description of the order provisions from which an exception is sought;

(iii) The name or a description sufficient to identify the covered article or the product or service provided by a source that is subject to the order from which an exception is sought;

(iv) Compelling justification for why an exception should be granted, such as the impact of the order on the agency's ability to fulfill its mission-critical functions, or considerations related to the national interest, including national security reviews, national security investigations, or national security agreements;

(v) Any alternative mitigations to be undertaken to reduce the risks addressed by the FASCSA order; and

(vi) Any other information requested by the issuing official.

40.204-2 Procedures on contracting for certain telecommunications and video surveillance services or equipment.

Identifying covered telecommunications equipment or services.

Prohibitions on purchasing equipment, systems, or services produced or provided by entities identified in paragraphs (1) and (2) of the definition of _covered telecommunications equipment or services_ (including known subsidiaries or affiliates) at 40.201 will be recorded in SAM (see 9.404).

(b) Prohibitions on purchasing equipment, systems, or services produced or provided by entities identified in paragraph (4) of the definition of _covered telecommunications equipment or services_ (including known subsidiaries or affiliates) at 40.201 are recorded by DoD in SAM (see 9.404).

40.204-3 Procedures on Sudan Prohibition.

Waivers.

(1) The President may waive the certification within the provision at 52.240-90(e) on a case-by-case basis if the President determines and certifies in writing to the appropriate congressional committees that it is in the national interest to do so.

(2) An agency seeking waiver of the requirement must submit the request to the Administrator of the Office of Federal Procurement Policy (OFPP), allowing sufficient time for review and approval. Upon receipt of the waiver request, OFPP must consult with the President's National Security Council and the Department of State to assess foreign policy aspects of making a national interest recommendation

(3) Agencies may request a waiver on an individual or class basis; however, waivers are not indefinite and can be cancelled if warranted.

(i) A class waiver may be requested only when the class of supplies is not available from any other source and it is in the national interest.

(ii) Prior to submitting the waiver request, the request must be reviewed and cleared by the agency head.

(iii) All waiver requests must include the following information:

(A) Agency name and point of contact name, telephone number, and email address;

(B) Offeror's name, complete mailing address, and point of contact name, telephone number, and email address;

(C) Description/nature of product or service;

(D) The total price and length of the contract;

(E) Justification, with market research demonstrating that no other offeror can provide the product or service and stating why the product or service must be procured from this offeror, as well as why it is in the national interest for the President to waive the prohibition on contracting with this offeror that conducts restricted business operations in Sudan, including consideration of foreign policy aspects identified in consultation(s) pursuant to 40.204-3(a)(2);

(F) Documentation regarding the offeror's past performance and integrity;

(G) Information regarding the offeror's relationship or connection with other firms that conduct prohibited business operations in Sudan; and

(H) Any humanitarian efforts engaged in by the offeror, the human rights impact of doing business with the offeror for which the waiver is requested, and the extent of the offeror's business operations in Sudan.

(4) The consultation in 40.204-3(a)(2) and the information in 40.204-3(a)(3)(iii) will be considered in determining whether to recommend that the President waive the

certification within the provision at 52.240-90(e). In accordance with section 6(c) of the Sudan Accountability and Divestment Act of 2007, OFPP will semiannually submit a report to Congress, on April 15th and October 15th, on the waivers granted.

(b) Remedies. Upon the determination of a false certification within the provision at 52.240-90(e)_

(1) The contracting officer may terminate the contract;

(2) The suspending and debarring official may suspend the contractor in accordance with the procedures in part 9; and

(3) The suspending and debarring official may debar the contractor for a period not to exceed 3 years in accordance with the procedures in part 9.

40.204-4 Procedures on Iran Prohibitions.

Waivers.

(1) An agency seeking a waiver of the representation and certifications in the provision at 52.240-90(f) or the prohibition in the clause at 52.240-91(d)(4), consistent with section 6(b)(5) of the Iran Sanctions Act or 22 U.S.C. 8551(b), respectively, and the Presidential Memorandum of September 23, 2010 (75 FR 67025), must submit the request to the Office of Federal Procurement Policy, allowing sufficient time for review and approval.

(2) Agencies may request a waiver on an individual or class basis; however, waivers are not indefinite and can be cancelled, if warranted.

(i) A class waiver may be requested only when the class of supplies or equipment is not available from any other source and it is in the national interest.

(ii) Prior to submitting the waiver request, the request must be reviewed and cleared by the agency head.

(3) In general, all waiver requests should include the following information:

(i) Agency name and point of contact name, telephone number, and email address.

(ii) Offeror's name, complete mailing address, and point of contact name, telephone number, and email address.

(iii) Description/nature of product or service.

(iv) The total price and length of the contract.

(v) Justification, with market research demonstrating that no other offeror can provide the product or service and stating why the product or service must be procured from this offeror.

(A) If the offeror exports 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, provide rationale why it is in the national interest for the President to waive the prohibition on contracting with this offeror, as required by 22 U.S.C. 8551(b).

(B) If the offeror conducts activities for which sanctions may be imposed under section 5 of the Iran Sanctions Act or engages in any transaction that exceeds the certification transaction threshold within the provision at 52.240-90(f)(1)(iii) 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, provide rationale why it is essential to the national security interests of the United States for the President to waive the prohibition on contracting with this offeror, as required by section 6(b)(5) of the Iran Sanctions Act.

(vi) Documentation regarding the offeror's past performance and integrity.

(vii) Information regarding the offeror's relationship or connection with other firms that_

(A) Export 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;

(B) Conduct activities for which sanctions may be imposed under section 5 of the Iran Sanctions Act; or

(C) Conduct any transaction that exceeds the certification transaction threshold within the provision at 52.240-90(f)(1)(iii) 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.

(viii) Describe _

(A) The sensitive technology and the entity or individual to which it was exported (i.e., the government of Iran or an entity or individual owned or controlled by, or acting on behalf or at the direction of, the government of Iran);

(B) The activities in which the offeror is engaged for which sanctions may be imposed under section 5 of the Iran Sanctions Act; or

(C) The transactions that exceed the certification transaction threshold within the provision at 52.240-90(f)(1)(iii) 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.

(b) Remedies. Upon the determination of a false certification within the provision at 52.240-90(f)(1)(ii) or at 52.240-90(f)(1)(iii), the agency must take one or more of the following actions:

(1) The contracting officer terminates the contract in accordance with procedures in part 49, or for commercial products and commercial services, see part 12.

(2) The suspending and debarring official suspends the contractor in accordance with the procedures in part 9.

(3) The suspending and debarring official debars the contractor for a period of at least two years in accordance with the procedures in part 9.

40.205 Solicitation provision and contract clause.

(a) Insert the provision at 52.240-90, Security Prohibitions and Exclusions Representations and Certifications, in all solicitations.

(b) Except as prescribed in paragraph (c), insert the clause at 52.240-91, Security Prohibitions and Exclusions, in all solicitations and contracts.

(c) Insert the clause with its Alternate I in-

(1) Federal Supply Schedules, Governmentwide acquisition contracts, and multi-agency contracts; and

(2) Where the program office or the requiring activity instructs the contracting officer to select specific types of FASCSA orders.

Subpart 40.3 - Safeguarding Information

40.300 Scope.

(a) This subpart provides policies and procedures for safeguarding classified information and Federal contract information.

(b) Part 27, Patents, Data, and Copyrights, contains policy and procedures for safeguarding classified information in patent applications and patents.

40.301 Definitions.

As used in this subpart:

Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as that on public Web sites) or simple transactional information, such as that necessary to process payments.

Information means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

Safeguarding means measures or controls that are prescribed to protect information systems.

40.302 Safeguarding classified information within industry.

40.302-1 National industrial security program.

This section provides policies and procedures to implement the National Industrial Security Program according to Executive Order 12829, January 6, 1993 (58 FR 3479, January 8, 1993), titled _National Industrial Security Program_ (NISP). Executive Order 12829 amends Executive Order 10865, February 20, 1960 (25 FR 1583, February 25, 1960), entitled 'safeguarding Classified Information Within Industry,_ as amended by Executive Order 10909, January 17, 1961 (26 FR 508, January 20, 1961). This program safeguards Federal Government classified information. The following publications implement the program:

(a)National Industrial Security Program Operating Manual (NISPOM) (32 CFR part 117).

(b) DoD Manual 5220.22, Volume 2, National Industrial Security Program: Industrial Security Procedures for Government Activities.

40.302-2 Responsibilities of contracting officers.

(a) Review all proposed solicitations to determine whether offerors or contractors may require access to classified information.

(b) Nondefense agencies that have industrial security services agreements with the Department of Defense (DoD) and DoD components must use the Contract Security Classification Specification, DD Form 254. The contracting officer or authorized agency representative is the approving official for the DD Form 254 associated with the prime contract and must ensure the DD Form 254 is properly prepared, distributed by and coordinated with requirements and security personnel, according to agency procedures.

40.302-3 Contract clause.

(a) Insert the clause at 52.240-92, Security Requirements, in solicitations and contracts when the contract may require access to classified information.

(b) If a cost contract for research and development with an educational institution is considered, use the clause with its Alternate I.

(c) If a construction or architect-engineer contract where employee identification is required for security reasons is being considered, use the clause with its Alternate II.

40.303 Basic safeguarding of covered contractor information systems.

40.303-1 Applicability.

This section applies to all acquisitions, including acquisitions of commercial products or commercial services, other than commercially available off-the-shelf items, when a contractor's information system may contain Federal contract information.

40.303-2 Contract clause.

Insert the clause at 52.240-93, Basic Safeguarding of Covered Contractor Information Systems, in solicitations and contracts when the contractor or a subcontractor at any tier may have Federal contract information residing in or moving through its information system.

Part 52 - Solicitation Provisions and Contract Clauses

52.240 [Reserved]

52.240-1 [Reserved]

52.240-90 Security Prohibitions and Exclusions Representations and Certifications.

As prescribed in 40.205(a), insert the following provision:

Security Prohibitions and Exclusions Representations and Certifications (NOV 2025)

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

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

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

Marginalized populations of Sudan means-

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

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

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

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

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

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

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

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

(6) Have been voluntarily suspended.

Sensitive technology-

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

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

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

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

(b) *Procedures*.

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

(2) *FASCSA Orders*.

(i) The Offeror shall search in SAM for the phrase "FASCSA order" for any covered article, or any products or services produced or provided by a source, if there is an applicable

FASCSA order described in paragraph (e)(1) 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) If a Department of Defense contracting office, the offeror shall submit the disclosure to the website at https://dibnet.dod.mil.

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

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

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

(End of provision)

52.240-91 Security Prohibitions and Exclusions.

As prescribed in 40.205(b), insert the following clause:

Security Prohibitions and Exclusions (Date)

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

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

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

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

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

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

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

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

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

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

Covered telecommunications equipment or services means-

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

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

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

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

Critical technology means-

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

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

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

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

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

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

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

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

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

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

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

order.

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

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

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

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

(i) Of that equipment; or

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

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

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

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

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

(2) The Central Intelligence Agency;

(3) The National Security Agency;

(4) The Defense Intelligence Agency;

(5) The National Geospatial-Intelligence Agency;

(6) The National Reconnaissance Office;

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

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

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

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

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

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

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

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

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

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

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

Kaspersky Lab-covered entity means-

(1) Kaspersky Lab;

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

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

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

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

(1) The function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a

system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(1) Prohibition. The Contractor is prohibited from-

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

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

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

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

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

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

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

(i) Unless an applicable waiver has been issued by the Government, the Contractor cannot

use any equipment, systems, or services that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system (paragraph (a)(1)(B) of section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232)).

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

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

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

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

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

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

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

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

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

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

(4) *Iran prohibitions*.

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

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

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

(iv) Unless an exception applies or the Government grants a waiver, contractors are prohibited from knowingly engaging in any significant transaction (i.e., over $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) If a Department of Defense contracting office, the Contractor shall report to the website at https://dibnet.dod.mil.

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

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

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

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

(i) *New FASCSA orders report*.

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

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

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

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

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

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

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

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

(End of clause)

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

(e) *Governmentwide exclusion and removal orders*.

(1) Contractors are prohibited from providing or using as part of the performance of the contract any covered article, or any products or services produced or provided by a source, if the covered article or the source is prohibited by any applicable FASCSA orders identified by the checkbox(es) in this paragraph (e)(1). [*Contracting Officer must select either "yes" or "no" for each of the following types of FASCSA orders*:]

Yes □ No □ DHS FASCSA Order

Yes □ No □ DoD FASCSA Order

Yes □ No □ DNI FASCSA Order

52.240-92 Security Requirements.

As prescribed in 40.302-3, insert the following clause:

Security Requirements (NOV 2025)

(a) This clause applies to the extent that this contract involves access to information classified Confidential, Secret, or Top Secret.

(b) The Contractor shall comply with-

(1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (32 CFR part 117); and

(2) Any revisions to that manual, notice of which has been furnished to the Contractor.

(c) If, after the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract must be subject to an equitable adjustment as if the changes were directed

under the Changes clause of this contract

(d)The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.

(e)A subcontractor requiring access to classified information under a contract shall be identified with a CAGE code on the DD Form 254. The Contractor shall require a subcontractor requiring access to classified information to provide its CAGE code with its name and location address or otherwise include it prominently in the proposal. Each location of subcontractor performance listed on the DD Form 254 is required to reflect a corresponding unique CAGE code for each listed location unless the work is being performed at a Government facility, in which case the agency location code shall be used. The CAGE code must be for that name and location address. Insert the word "CAGE" before the number. The CAGE code is required prior to award. The contractor shall ensure that subcontractors maintain their CAGE code(s) throughout the life of the contract.

(End of clause)

Alternate I (NOV 2025). If a cost contract for research and development with an educational institution is contemplated, add the following paragraphs (f), (g), and (h) to the basic clause:

(f)(1) If a change in security requirements, as provided in paragraphs (b) and (c), results in a change in the security classification of this contract or any of its elements from an unclassified status or a lower classification to a higher classification, or in more restrictive area controls than previously required, then the Contractor must exert every reasonable effort compatible with the Contractor's established policies to continue performing the work under the contract to comply with the change in security classification or requirements.

(2) If, despite reasonable efforts, the Contractor determines that continuing work under this contract is not practical because of the change in security classification or requirements, the Contractor shall notify the Contracting Officer in writing. Until the Contracting Officer resolves this problem, the Contractor shall continue safeguarding all classified material as required by this contract.

(g) After receiving the written notification, the Contracting Officer shall explore the circumstances surrounding the proposed change in security classification or requirements and must try to work out a mutually satisfactory method so the Contractor can continue doing the work under this contract.

(h) If, 15 days after receipt by the Contracting Officer of the notification of the Contractor's stated inability to proceed, the application to this contract of the change in security classification or requirements has not been withdrawn or a mutually satisfactory method for continuing performance of work under this contract has not been agreed upon, the

Contractor may request the Contracting Officer to terminate the contract in whole or in part. The Contracting Officer shall terminate the contract in whole or in part, as may be appropriate, and the termination must be deemed a termination under the terms of the Termination for the Convenience of the Government clause.

Alternate I (DATE). If employee identification is required for security or other reasons in a construction contract or architect-engineer contract, add the following paragraph (f) to the basic clause:

(f) The Contractor is responsible for furnishing to each employee, and for requiring each employee engaged on the work to display, such identification as may be approved and directed by the Contracting Officer. All prescribed identification shall immediately be delivered to the Contracting Officer, for cancellation upon the release of any employee. When required by the Contracting Officer, the Contractor shall obtain and submit fingerprints of all persons employed or to be employed on the project.

52.240-93 Basic Safeguarding of Covered Contractor Information Systems.

As prescribed in 40.303-2, insert the following clause:

Basic Safeguarding of Covered Contractor Information Systems (NOV 2025)

(a) Definitions. As used in this clause-

Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Federal contract information-

(1) Means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government; but

(2) Does not include information provided by the Government to the public (such as on public websites) or simple transactional information (such as information necessary to process payments).

Information means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

Safeguarding means measures or controls that are prescribed to protect information

systems.

(b) *Safeguarding requirements*.

(1) Basic requirements. The Contractor shall safeguard its covered contractor information systems by implementing, at minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(2) Other requirements. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal departments and agencies relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(c) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial products, other than commercially available off-the-shelf items, or commercial services), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

(End of clause)