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

40.204-3 Procedures on Sudan Prohibition.

40.204-4 Procedures on Iran Prohibitions.

40.205 Solicitation provision and contract clause.

Subpart 40.3 - Safeguarding Information

40.300 Scope.

40.301 Definitions.

40.302 Safeguarding classified information within industry.

40.302-1 National industrial security program.

40.~~202-8~~302-2 Responsibilities of contracting officers.

40.302-3 Contract clause.

40.303 Basic safeguarding of covered contractor information systems.

40.303-1 Applicability.

40.~~Subpart 40.3 - [Reserved]~~

~~Parent topic: Federal Acquisition Regulation~~303-2 Contract clause.

40.000 Scope of part.
(a) This part addresses broad security requirements that apply to acquisitions of products and services. It ~~prescribes~~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 ~~part 39 for security-related policies and procedures that only apply to ICT.~~

~~(c) See~~ parts ~~4,~~ 24~~,~~ and 46 for ~~additional~~more policies and procedures related to managing information security and supply chain security.

(~~d~~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 - ~~[Reserved]~~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
~~40.200 Scope of subpart.~~
~~(a) This subpart provides policies and procedures to implement security prohibitions and exclusions that restrict Federal agencies from procuring, obtaining, or using certain products, services, or sources.~~

~~(b) The following prohibitions and exclusions are implemented in this subpart:~~

~~(1) The American Security Drone Act of 2023, of the National Defense Authorization Act for Fiscal Year 2024 (Pub. L. 118-31, 41 U.S.C. 3901 note prec.), which provides a prohibition on the procurement and operation of unmanned aircraft systems.~~

~~(2) [Reserved]~~

~~(c) Additional security prohibitions and exclusions are found at subparts 4.20 through 4.23 and 25.7.~~

40.201 Definitions.
As used in this subpart~~:~~—

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

~~Unmanned aircraftmeans~~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 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.

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 ~~systemmeans~~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 Prohibition on the procurement and operation of unmanned aircraft systems manufactured or assembled by American Security Drone Act-covered foreign entities. s.~~
~~(a) Section 40.202 prescribes policies and procedures regarding the procurement and operation of unmanned aircraft systems, which includes unmanned aircraft (i.e., drones) and associated elements.~~

~~(b) The authorities in 40.202 expire on December 22, 2028 (section 1833 of Pub. L. 118-31, 41 U.S.C. 3901 note prec.).~~

~~40.202-1 Scope.~~

~~(a) Section 40.202 prescribes policies and procedures regarding the procurement and operation of unmanned aircraft systems, which includes unmanned aircraft (i.e., drones) and associated elements.~~

~~(b) The authorities in 40.203 expire on December 22, 2028 (section 1833 of Pub. L. 118-31, 41 U.S.C. 3901 note prec.).~~

40.202 Prohibitions.

~~40.~~202-2 Applicability.

~~Section 40.202 applies to all acquisitions, including contracts at or below the micro-purchase threshold and to contracts for commercial products or for commercial services.~~

~~40.~~202-3 Prohibition.

~~Unless an exemption, exception, or waiver applies (see 40.202-4, 40.202-5, and 40.202-6, respectively), executive~~ Agencies are prohibited from~~-~~

~~(a) Procuring a FASC-prohibited unmanned aircraft system (section 1823 and 1826 of Pub. L. 118-31, 41 U.S.C. 3901 note prec.). The prohibition includes extending or renewing a contract (e.g., exercising an option);~~

contracting, including renewing or extending contracts, with contractors that operate, provide, and/or use certain products or services that violate any of

~~(b) On or after December 22, 2025, procuring services for the operation of a FASC-prohibited unmanned aircraft system (section 1824 of Pub. L. 118-31, 41 U.S.C. 3901 note prec.). The prohibition includes extending or renewing a contract (e.g., exercising an option); and~~

~~(c) On or after December 22, 2025, using Federal funds for the procurement or operation of a FASC-prohibited unmanned aircraft system (section 1825 of Pub. L. 118-31, 41 U.S.C. 3901 note prec.).~~

~~40.~~202-4 Exemptions.

~~The prohibitions in 40.202 do not apply to~~ the following ~~(see sections 1823, 1824, and 1825 of Pub. L. 118-31, 41 U.S.C. 3901 note prec.):~~

~~(a) Department of Homeland Security, Department of Defense, Department of State, and the Department of Justice exemptions. The Secretary of Homeland Security, the Secretary of Defense, the Secretary of State, and the Attorney General are exempt from the prohibitions in 40.202 if the procurement or operation is required in the national interest of the United States and~~

prohibitions (see

~~(1) Is~~ for the sole purposes of research, evaluation, training, testing, or analysis for electronic warfare, information warfare operations, cybersecurity, or development of unmanned aircraft system or counter-unmanned aircraft system technology;

(2) Is for the sole purposes of conducting counterterrorism or counterintelligence activities, protective missions, or Federal criminal or national security investigations, including forensic examinations, or for electronic warfare, information warfare operations, cybersecurity, or development of an unmanned aircraft system or counter-unmanned aircraft system technology; or

(3) Is an unmanned aircraft system that, as procured or as modified after procurement but before operational use, can no longer transfer to, or download data from, an American Security Drone Act-covered foreign entity and otherwise poses no national security cybersecurity risks as determined by the exempting official, as described in agency procedures.

(b) Department of Transportation exemption. The Secretary of Transportation is exempt from the prohibitions in 40.202 if the operation or procurement is deemed to support the safe, secure, or efficient operation of the National Air Space System or maintenance of public safety.

(c) National Transportation Safety Board exemption. The National Transportation Safety Board, in consultation with the Secretary of Homeland Security, is exempt from the prohibitions, in 40.202 if the operation or procurement is necessary for the sole purpose of conducting safety investigations.

(d) National Oceanic and Atmospheric Administration (NOAA) exemption. The Administrator of NOAA, in consultation with the Secretary of Homeland Security, is exempt from the prohibitions of 40.202, if the operation or procurement for the purposes of meeting NOAA's science or management objectives or operational mission.

40.202-5 Exceptions.
The prohibitions in this section do not apply to the following (section 1832 of Pub. L. 118-31, 41 U.S.C. 3901 note prec.):

(a) Wildfire management operations and search and rescue operations exception. The prohibitions in section 40.202 do not apply to an appropriate Federal agency to the extent that an authorized official at the agency, in consultation with the Secretary of Homeland Security, determines that the procurement or operation is necessary for the purposes of supporting the full range of wildfire management operations or search and rescue operations.

(b) Intelligence activities exception. The prohibitions of 40.202 do not apply to any activity subject to the reporting requirements under title V of the National Security Act of 1947 (50 U.S.C. 3091 et seq.), any authorized intelligence activities of the United States, or any activity or procurement that supports an authorized intelligence activity.

(c) Tribal law enforcement or emergency service agency exception. The prohibitions in 40.202 do not apply to Tribal law enforcement or Tribal emergency service agencies to the extent that an authorized official at the agency, in consultation with the Secretary of Homeland Security, determines that the procurement or operation is necessary for the purposes of supporting the full range of law enforcement operations or search and rescue operations on Indian lands.

~~40.202-6 Waivers.~~

~~The head of the agency may waive the prohibitions under 40.202 on a case-by-case basis in accordance with agency procedures and based on the statutory waiver provisions (sections 1823, 1824, and 1825 of Pub. L. 118-31, 41 U.S.C. 3901 note prec.)~~

~~(a)With the approval of the Director of the Office of Management and Budget, after consultation with the FASC; and~~

~~(b)Upon notification to~~

~~(1) The Committee on Homeland Security and Governmental Affairs of the Senate;~~

~~(2) The Committee on Oversight and Accountability in the House of Representatives; and~~

~~(3) Other appropriate congressional committees of jurisdiction.~~

~~40.202-7 Procedures.~~

~~(a) Documenting exemptions, exceptions, or waivers. The contracting officer shall document the file with any exemption, exception, or waiver provided by the program office or requiring activity. Additionally, the contracting officer shall work with the program office or requiring activity to ensure the presence and scoping of any such exemptions, exceptions, or waivers are identified in the solicitation and resultant contract.~~

~~(b) Assessment of unmanned aircraft systems. Except where an exemption, exception, or waiver applies, the contracting officer shall work with the program office or requiring activity to review proposals to ensure they are not proposing delivery of a FASC-prohibited unmanned aircraft system. On or after December 22, 2025, this assessment shall expand to include review for not only proposed delivery, but also operation, of a FASC-prohibited unmanned aircraft system.~~

~~40.202-8 Contract clause.~~

~~Insert~~ 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) ~~1, Prohibition on~~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 Disclosures.
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 a contractor submits a report according to the clause at 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.

(a) 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.
(a)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.
(a)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 ~~and contracts~~.

(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 - ~~[Reserved]~~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.