to the close of the proceeding, for submitting a version of the document(s) proposed for public availability that reflects the requested deletion. The restricted access portion of the record will be placed in a separate file and the file will be clearly marked to avoid improper disclosure and to identify it as a portion of the official record in the proceedings. The ALJ may act at any time to permit material that becomes declassified or unrestricted through passage of time to be transferred to the unrestricted access portion of the record.

(c) *Availability of documents*—(1) *Scope*. All NOVAs and draft NOVAs, answers, settlement agreements, decisions and orders disposing of a case will be displayed on the BIS Freedom of Information Act (FOIA) Web site, at *http://www.bis.doc.gov/foia,* which is maintained by the Office of Administration, Bureau of Industry and Security, U.S. Department of Commerce. The Office of Administration does not maintain a separate inspection facility. The complete record for decision, as defined in paragraphs (a) and (b) of this section will be made available on request.

(2) *Timing*. The record for decision will be available only after the final administrative disposition of a case. Parties may seek to restrict access to any portion of the record under paragraph (b) of this section.

§ 785.19 Payment of final assessment.

(a) *Time for payment*. Full payment of the civil penalty must be made within 30 days of the effective date of the order or within such longer period of time as may be specified in the order. Payment shall be made in the manner specified in the NOVA.

(b) *Enforcement of order*. The government party may, through the Attorney General, file suit in an appropriate district court if necessary to enforce compliance with a final order issued under the APR. This suit will include a claim for interest at current prevailing rates from the date of expiration of the 60-day period referred to in §785.16(d), or the date of the final order, as appropriate.

(c) *Offsets*. The amount of any civil penalty imposed by a final order may be deducted from any sum(s) owed by the United States to a respondent.

§ 785.20 Reporting a violation.

If a person learns that a violation of the Additional Protocol, the Act, or the APR has occurred or may occur, that person may notify: Office of Export Enforcement, Bureau of Industry and Security, U.S. Department of Commerce, 14th Street and Constitution Avenue, NW., Room H–4520, Washington, DC 20230; Tel: (202) 482–1208; Facsimile: (202) 482–0964.

PART 786—RECORDS AND RECORDKEEPING

Sec.
786.1 Inspection of records.
786.2 Recordkeeping.
786.3 Destruction or disposal of records.

AUTHORITY: United States Additional Protocol Implementation Act of 2006, Pub. Law No. 109–401, 120 Stat. 2726 (December 18, 2006) (to be codified at 22 U.S.C. 8101–8181); Executive Order 13458 (February 4, 2008).

SOURCE: 73 FR 65128, Oct. 31, 2008, unless otherwise noted.

§ 786.1 Inspection of records.

Upon request by BIS, you must permit access to and copying of any record relating to compliance with the requirements of the APR. This requires that you make available the equipment and, if necessary, knowledgeable personnel for locating, reading, and reproducing any record. Copies may be necessary to facilitate IAEA Team review of documents during complementary access. The IAEA Team may not remove these documents from the location without BIS authorization (see §784.3(j)(2) of the APR).

§ 786.2 Recordkeeping.

(a) *Requirements*. Each person and location required to submit a report or correspondence under parts 782 through 784 of the APR must retain all supporting materials and documentation used to prepare such report or correspondence.

(b) *Three year retention period*. All supporting materials and documentation required to be kept under paragraph (a) of this section must be retained for three years from the due

date of the applicable report or for three years from the date of submission of the applicable report, whichever is later. Due dates for reports and correspondence are indicated in parts 782 through 784 of the APR.

(c) *Location of records.* Records retained under this section must be maintained at the location or must be accessible at the location for purposes of complementary access at the location by IAEA Teams.

(d) *Reproduction of original records.* (1) You may maintain reproductions instead of the original records, provided all of the requirements of paragraph (b) of this section are met.

(2) If you must maintain records under this part, you may use any photostatic, miniature photographic, micrographic, automated archival storage, or other process that completely, accurately, legibly and durably reproduces the original records (whether on paper, microfilm, or through electronic digital storage techniques). The process must meet all of the following requirements, which are applicable to all systems:

(i) The system must be capable of reproducing all records on paper.

(ii) The system must record and be able to reproduce all marks, information, and other characteristics of the original record, including both obverse and reverse sides (unless blank) of paper documents in legible form.

(iii) When displayed on a viewer, monitor, or reproduced on paper, the records must exhibit a high degree of legibility and readability. For purposes of this section, legible and legibility mean the quality of a letter or numeral that enable the observer to identify it positively and quickly to the exclusion of all other letters or numerals. Readable and readability mean the quality of a group of letters or numerals being recognized as complete words or numbers.

(iv) The system must preserve the initial image (including both obverse and reverse sides, unless blank, of paper documents) and record all changes, who made them and when they were made. This information must be stored in such a manner that none of it may be altered once it is initially recorded.

(v) You must establish written procedures to identify the individuals who are responsible for the operation, use and maintenance of the system.

(vi) You must keep a record of where, when, by whom, and on what equipment the records and other information were entered into the system.

(3) *Requirements applicable to a system based on digital images.* For systems based on the storage of digital images, the system must provide accessibility to any digital image in the system. The system must be able to locate and reproduce all records according to the same criteria that would have been used to organize the records had they been maintained in original form.

(4) *Requirements applicable to a system based on photographic processes.* For systems based on photographic, photostatic, or miniature photographic processes, the records must be maintained according to an index of all records in the system following the same criteria that would have been used to organize the records had they been maintained in original form.

§ 786.3 Destruction or disposal of records.

If BIS or any other authorized U.S. government agency makes a formal or informal request for a certain record or records, such record or records may not be destroyed or disposed of without the written authorization of the requesting entity.

PARTS 787–789 [RESERVED]

SUBCHAPTER E—INFORMATION AND COMMUNICATIONS TECHNOLOGY AND SERVICES REGULATIONS

PART 790 [RESERVED]

PART 791—SECURING THE INFORMATION AND COMMUNICATIONS TECHNOLOGY AND SERVICES SUPPLY CHAIN

Subpart A—General

Subpart B—Review of ICTS Transactions

Subpart C—Enforcement

AUTHORITY: 50 U.S.C. 1701 *et seq.;* 50 U.S.C. 1601 *et seq.;* E.O. 13873, 84 FR 22689; E.O. 14034, 86 FR 31423

SOURCE: 86 FR 4923, Jan. 19, 2021, unless otherwise noted. Redesignated at 89 FR 58265, July 18, 2024.

EFFECTIVE DATE NOTE: At 89 FR 96892, Dec. 6, 2024, part 791 was amended by: 1) removing the text ''initial determination'' wherever it appears, and adding, in its place, the text ''Initial Determination'', and 2) removing the text ''final determination'' wherever it appears, and adding, in its place, the text ''Final Determination'', effective Feb. 4, 2025.

Subpart A—General

§ 791.1 Purpose.

(a) This part sets forth the procedures by which the Secretary may:

(1) Determine whether any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service, including but not limited to connected software applications, (ICTS Transaction) that has been designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries poses certain undue or unacceptable risks as identified in the Executive Order. For purposes of these regulations, the Secretary will consider ICTS to be designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction of a foreign adversary where such a person operates, manages, maintains, or services the ICTS;

(2) Issue a determination to prohibit an ICTS Transaction;

(3) Direct the timing and manner of the cessation of the ICTS Transaction;

(4) Consider factors that may mitigate the risks posed by the ICTS Transaction.

(b) The Secretary will evaluate ICTS Transactions under this rule, which include, but are not limited to, classes of transactions, on a case-by-case basis. The Secretary, in consultation with appropriate agency heads specified in Executive Order 13873 and other relevant governmental bodies, as appropriate, shall make an initial determination as to whether to prohibit a given ICTS Transaction or propose mitigation measures, by which the ICTS Transaction may be permitted. Parties may submit information in response to the initial determination, including a response to the initial determination and any supporting materials and/or proposed measures to remediate or mitigate the risks identified in the initial determination as posed by the ICTS Transaction at issue. Upon consideration of the parties' submissions, the Secretary will issue a final determination prohibiting the transaction, not prohibiting the transaction, or permitting the transaction subject to the

adoption of measures determined by the Secretary to sufficiently mitigate the risks associated with the ICTS Transaction. The Secretary shall also engage in coordination and information sharing, as appropriate, with international partners on the application of this part.

[88 FR 39357, June 16, 2023]

EFFECTIVE DATE NOTE: At 89 FR 96892, Dec. 6, 2024, §791.1 was amended by revising paragraph (a)(1), effective Feb. 4, 2025. For the convenience of the user, the revised text is set forth as follows:

§ 791.1 Purpose.

(a) * * *

(1) Determine whether any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service, including but not limited to connected software applications, (ICTS Transaction) that has been designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries poses certain undue or unacceptable risks as identified in the Executive Order 13873. For purposes of these regulations, the Secretary will consider information and communications technology and services (ICTS) to be designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction of a foreign adversary where such a person operates, manages, maintains, repairs, updates, or services the ICTS;

* * * * *

§ 791.2 Definitions.

Appropriate agency heads means the Secretary of the Treasury, the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the United States Trade Representative, the Director of National Intelligence, the Administrator of General Services, the Chairman of the Federal Communications Commission, and the heads of any other executive departments and agencies the Secretary determines is appropriate.

Commercial item has the same meaning given to it in Federal Acquisition Regulation (48 CFR part 2.101).

Connected software application means software, a software program, or a group of software programs, that is designed to be used on an end-point computing device and includes as an integral functionality, the ability to collect, process, or transmit data via the internet.

Department means the United States Department of Commerce.

End-point computing device means a device that can receive or transmit data and includes as an integral functionality the ability to collect or transmit data via the internet.

Entity means a partnership, association, trust, joint venture, corporation, group, subgroup, or other non-U.S. governmental organization.

Executive Order means Executive Order 13873, May 15, 2019, ''Securing the Information and Communications Technology and Services Supply Chain''.

Foreign adversary means any foreign government or foreign non-government person determined by the Secretary to have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons.

ICTS Transaction means any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs, or the platforming or data hosting of applications for consumer download. An ICTS Transaction includes any other transaction, the structure of which is designed or intended to evade or circumvent the application of the Executive Order. The term ICTS Transaction includes a class of ICTS Transactions.

IEEPA means the International Emergency Economic Powers Act (50 U.S.C. 1701, *et seq.*).

Information and communications technology or services or *ICTS* means any hardware, software, including connected software applications, or other product or service, including cloud-computing services, primarily intended to fulfill or enable the function of information or data processing, storage,

retrieval, or communication by electronic means (including electromagnetic, magnetic, and photonic), including through transmission, storage, or display.

Party or parties to a transaction means a person engaged in an ICTS Transaction, including the person acquiring the ICTS and the person from whom the ICTS is acquired. Party or parties to a transaction include entities designed, or otherwise used with the intention, to evade or circumvent application of the Executive Order. For purposes of this rule, this definition does not include common carriers, except to the extent that a common carrier knew or should have known (as the term ''knowledge'' is defined in 15 CFR 772.1) that it was providing transportation services of ICTS to one or more of the parties to a transaction that has been prohibited in a final written determination made by the Secretary or, if permitted subject to mitigation measures, in violation of such mitigation measures.

Person means an individual or entity.

Person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary means any person, wherever located, who acts as an agent, representative, or employee, or any person who acts in any other capacity at the order, request, or under the direction or control, of a foreign adversary or of a person whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized in whole or in majority part by a foreign adversary; any person, wherever located, who is a citizen or resident of a nation-state controlled by a foreign adversary; any corporation, partnership, association, or other organization organized under the laws of a nation-state controlled by a foreign adversary; and any corporation, partnership, association, or other organization, wherever organized or doing business, that is owned or controlled by a foreign adversary.

Secretary means the Secretary of Commerce or the Secretary's designee.

Sensitive personal data means:

(1) Personally-identifiable information, including:

(i) Financial data that could be used to analyze or determine an individual's financial distress or hardship;

(ii) The set of data in a consumer report, as defined under 15 U.S.C. 1681a, unless such data is obtained from a consumer reporting agency for one or more purposes identified in 15 U.S.C. 1681b(a);

(iii) The set of data in an application for health insurance, long-term care insurance, professional liability insurance, mortgage insurance, or life insurance;

(iv) Data relating to the physical, mental, or psychological health condition of an individual;

(v) Non-public electronic communications, including email, messaging, or chat communications, between or among users of a U.S. business's products or services if a primary purpose of such product or service is to facilitate third-party user communications;

(vi) Geolocation data collected using positioning systems, cell phone towers, or WiFi access points such as via a mobile application, vehicle GPS, other onboard mapping tool, or wearable electronic device;

(vii) Biometric enrollment data including facial, voice, retina/iris, and palm/fingerprint templates;

(viii) Data stored and processed for generating a Federal, State, Tribal, Territorial, or other government identification card;

(ix) Data concerning U.S. Government personnel security clearance status; or

(x) The set of data in an application for a U.S. Government personnel security clearance or an application for employment in a position of public trust; or

(2) Genetic information, which includes the results of an individual's genetic tests, including any related genetic sequencing data, whenever such results, in isolation or in combination with previously released or publicly available data, constitute identifiable data. Such results shall not include data derived from databases maintained by the U.S. Government and routinely provided to private parties for purposes of research. For purposes of this paragraph, ''genetic test'' shall

have the meaning provided in 42 U.S.C. 300gg–91(d)(17).

Undue or unacceptable risk means those risks identified in Section 1(a)(ii) of the Executive Order.

United States person means any United States citizen; any permanent resident alien; or any entity organized under the laws of the United States or any jurisdiction within the United States (including such entity's foreign branches).

Via the internet means using internet protocols to transmit data, including, but not limited to, transmissions by cable, telephone lines, wireless methods, satellites, or other means.

[86 FR 4923, Jan. 19, 2021, as amended at 88 FR 39357, June 16, 2023]

EFFECTIVE DATE NOTE: At 89 FR 96892, Dec. 6, 2024, § 791.2 was amended by:

1. Revising the definition of ''Appropriate agency heads'',
2. Adding in alphabetical order definitions for ''Covered ICTS Transaction'', ''Dealing in'', and ''Importation'', and
3. Revising the definitions of ''Party or parties to a Transaction'', ''Person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary'', ''Secretary'', and ''United States Person'', effective Feb. 4, 2025.

For the convenience of the user, the added and revised text is set forth as follows:

§ 791.2 Definitions.

Appropriate agency heads means the Secretary of the Treasury, the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the United States Trade Representative, the Director of National Intelligence, the Administrator of General Services, the Chairman of the Federal Communications Commission, and the heads of any other executive departments and agencies the Secretary determines is appropriate, or their designees.

* * * * *

Covered ICTS Transaction means an ICTS Transaction or a class of ICTS Transactions that meets the criteria set forth in § 791.3.

Dealing in means the activity of buying, selling, reselling, receiving, licensing, or acquiring ICTS, or otherwise doing or engaging in business involving the conveyance of ICTS.

* * * * *

Importation means the process or activity of bringing foreign ICTS to or into the United States, regardless of the means of conveyance, including via electronic transmission.

* * * * *

Party or parties to a Transaction means a person or persons engaged in an ICTS Transaction or class of ICTS Transactions, including, but not limited to the following: designer, developer, provider, buyer, purchaser, seller, transferor, licensor, broker, acquiror, intermediary (including consignee), and end user. Party or parties to a Transaction include entities designed, or otherwise used with the intention, to evade or circumvent application of the Executive Order. For purposes of this rule, this definition does not include common carriers, except to the extent that a common carrier knew or should have known (as the term ''knowledge'' is defined in 15 CFR 772.1) that it was providing transportation services of ICTS to one or more of the parties to a Transaction that has been prohibited in a final written determination made by the Secretary or, if permitted subject to mitigation measures, in violation of such mitigation measures.

* * * * *

Person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary means:

(1) Any person, wherever located, who acts as an agent, representative, or employee, or any person who acts in any other capacity at the order, request, or under the direction or control, of a foreign adversary or of a person whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized in whole or in majority part by a foreign adversary;

(2) Any person, wherever located, who is a citizen or resident of a foreign adversary or a country controlled by a foreign adversary, and is not a United States citizen or permanent resident of the United States;

(3) Any corporation, partnership, association, or other organization with a principal place of business in, headquartered in, incorporated in, or otherwise organized under the laws of a foreign adversary or a country controlled by a foreign adversary; or

(4) Any corporation, partnership, association, or other organization, wherever organized or doing business, that is owned or controlled by a foreign adversary, to include circumstances in which any person identified in paragraphs (1) through (3) of this definition possesses the power, direct or indirect, whether or not exercised, through the ownership of a majority or a dominant minority of the total outstanding voting interest in an entity, board representation, proxy voting, a

special share, contractual arrangements, formal or informal arrangements to act in concert, or other means, to determine, direct, or decide important matters affecting an entity.

Secretary means the Secretary of Commerce or the Secretary's designee, including for example the Under Secretary of Commerce for Industry and Security or the Executive Director of the Office of Information and Communications Technology and Services.

* * * * *

United States person means any United States citizen; any permanent resident alien; any entity organized under the laws of the United States or any jurisdiction within the United States (including such entity's foreign branches); or any person in the United States.

* * * * *

§ 791.3 Scope of Covered ICTS Transactions.

(a) This part applies only to an ICTS Transaction that:

(1) Is conducted by any person subject to the jurisdiction of the United States or involves property subject to the jurisdiction of the United States;

(2) Involves any property in which any foreign country or a national thereof has an interest (including through an interest in a contract for the provision of the technology or service);

(3) Is initiated, pending, or completed on or after January 19, 2021, regardless of when any contract applicable to the transaction is entered into, dated, or signed or when any license, permit, or authorization applicable to such transaction was granted. Any act or service with respect to an ICTS Transaction, such as execution of any provision of a managed services contract, installation of software updates, or the conducting of repairs, that occurs on or after January 19, 2021 may be deemed an ICTS Transaction within the scope of this part, even if the contract was initially entered into, or the activity commenced, prior to January 19, 2021; and

(4) Involves one of the following ICTS:

(i) ICTS that will be used by a party to a transaction in a sector designated as critical infrastructure by Presidential Policy Directive 21—Critical Infrastructure Security and Resilience, including any subsectors or subsequently designated sectors;

(ii) Software, hardware, or any other product or service integral to:

(A) Wireless local area networks, including:

(*1*) Distributed antenna systems; and

(*2*) Small-cell or micro-cell base stations;

(B) Mobile networks, including:

(*1*) eNodeB based stations;

(*2*) gNodeB or 5G new radio base stations;

(*3*) NodeB base stations;

(*4*) Home location register databases;

(*5*) Home subscriber servers;

(*6*) Mobile switching centers;

(*7*) Session border controllers; and

(*8*) Operation support systems;

(C) Satellite payloads, including:

(1) Satellite telecommunications systems;

(*2*) Satellite remote sensing systems; and

(*3*) Satellite position, navigation, and timing systems;

(D) Satellite operations and control, including:

(*1*) Telemetry, tracking, and control systems;

(*2*) Satellite control centers;

(*3*) Satellite network operations;

(*4*) Multi-terminal ground stations; and

(*5*) Satellite uplink centers;

(E) Cable access points, including:

(*1*) Core routers;

(*2*) Core networks; and

(*3*) Core switches;

(F) Wireline access points, including:

(*1*) Access infrastructure datalinks; and

(*2*) Access infrastructure digital loops;

(G) Core networking systems, including:

(*1*) Core infrastructure synchronous optical networks and synchronous digital hierarchy systems;

(*2*) Core infrastructure dense wavelength division multiplexing or optical transport network systems;

(*3*) Core infrastructure internet protocol and internet routing systems;

(*4*) Core infrastructure content delivery network systems;

(*5*) Core infrastructure internet protocol and multiprotocol label switching systems;

(*6*) Data center multiprotocol label switching routers; and

(*7*) Metropolitan multiprotocol label switching routers; or

(H) Long- and short-haul networks, including:

(*1*) Fiber optical cables; and

(*2*) Repeaters;

(iii) Software, hardware, or any other product or service integral to data hosting or computing services, to include software-defined services such as virtual private servers, that uses, processes, or retains, or is expected to use, process, or retain, sensitive personal data on greater than one million U.S. persons at any point over the twelve (12) months preceding an ICTS Transaction, including:

(A) Internet hosting services;

(B) Cloud-based or distributed computing and data storage;

(C) Managed services; and

(D) Content delivery services;

(iv) Any of the following ICTS products, if greater than one million units have been sold to U.S. persons at any point over the twelve (12) months prior to an ICTS Transaction:

(A) Internet-enabled sensors, webcams, and any other end-point surveillance or monitoring device;

(B) Routers, modems, and any other home networking device; or

(C) Drones or any other unmanned aerial system;

(v) Software designed primarily to enable connecting with and communicating via the internet, which is accessible through cable, telephone line, wireless, or satellite or other means, that is in use by greater than one million U.S. persons at any point over the twelve (12) months preceding an ICTS Transaction, including:

(A) Desktop applications;

(B) Mobile applications;

(C) Gaming applications;

(D) Web-based applications; and

(E) Connected software applications; or

(vi) ICTS integral to:

(A) Artificial intelligence and machine learning;

(B) Quantum key distribution;

(C) Quantum computing;

(D) Drones;

(E) Autonomous systems; or

(F) Advanced Robotics.

(b) This part does not apply to an ICTS Transaction that:

(1) Involves the acquisition of ICTS items by a United States person as a party to a transaction authorized under a U.S. government-industrial security program; or

(2) The Committee on Foreign Investment in the United States (CFIUS) is actively reviewing, or has reviewed, as a covered transaction or covered real estate transaction or as part of such a transaction under section 721 of the Defense Production Act of 1950, as amended, and its implementing regulations.

(c) Notwithstanding the exemption in paragraph (b)(2) of this section, ICTS Transactions conducted by parties to transactions reviewed by CFIUS that were not part of the covered transaction or covered real estate transaction reviewed by CFIUS remain fully subject to this part.

[86 FR 4923, Jan. 19, 2021, as amended at 88 FR 39358, June 16, 2023]

EFFECTIVE DATE NOTE: At 89 FR 96893, Dec. 6, 2024, §791.3 was amended by revising paragraphs (a)(2), (4) and (b), and removing paragraph (c), effective Feb. 4, 2025. For the convenience of the user, the revised text is set forth as follows:

§ 791.3 Scope of Covered ICTS Transactions.

(a) * * *

* * * * *

(2) Involves any property in which any foreign country or a national thereof has any interest of any nature whatsoever, whether direct or indirect (including through an interest in a contract for the provision of the technology or service);

* * * * *

(4) Involves ICTS and software, hardware, or any other product or service integral to one of the following:

(i) Information and communications hardware and software, including

(A) Wireless local area networks;

(B) Mobile networks;

(C) Satellite payloads;

(D) Satellite operations and control;

(E) internet-enabled sensors, cameras, and any other end-point surveillance or monitoring device, or any device that includes these components such as drones;

(F) Routers, modems, and any other networking devices;
(G) Cable access points;
(H) Wireline access points;
(I) Core networking systems;
(J) Long- and short-haul networks;
(ii) Data hosting, computing or storage, including software, hardware, or any other product or service integral to data hosting or computing services, including software-defined services such as virtual private servers, that uses, processes, or retains, or is expected to use, process, or retain, sensitive personal data of United States persons, including:
(A) internet hosting services;
(B) Cloud-based or distributed computing and data storage;
(C) Managed services; and
(D) Content delivery services;
(iii) Connected software applications, including software designed primarily to enable connecting with and communicating via the internet, which is accessible through cable, telephone line, wireless, or satellite or other means, that is in use by United States persons at any point over the twelve (12) months preceding an ICTS Transaction, including connected software applications, such as but not limited to, desktop applications, mobile applications, gaming applications, and web-based applications;
(iv) Critical infrastructure, including any subsectors of the chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government services and facilities, health care and public health, information technology, nuclear reactors, materials, and waste, transportation systems, and water and wastewater systems sectors, and
(v) Critical and emerging technologies, including advanced network sensing and signature management; advanced computing; artificial intelligence; clean energy generation and storage; data privacy, data security, and cybersecurity technologies; highly automated, autonomous, and uncrewed systems and robotics; integrated communication and networking technologies; positioning, navigation, and timing technologies; quantum information and enabling technologies; semiconductors and microelectronics; and biotechnology.
(b) The Secretary will not continue review of an ICTS Transaction under §791.103 if the Secretary finds that:
(1) The ICTS Transaction involves the acquisition of ICTS items by a United States person as a party to a transaction authorized under a U.S. government-industrial security program; or
(2) The Committee on Foreign Investment in the United States (CFIUS) is conducting a review, investigation, or assessment, or has concluded action on, the specific ICTS Transaction as a covered transaction under section 721(a)(4) of the Defense Production Act of 1950, as amended, and its implementing regulations.

§ 791.4 Determination of foreign adversaries.

(a) The Secretary has determined that the following foreign governments or foreign non-government persons have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons and, therefore, constitute foreign adversaries solely for the purposes of the Executive Order, this rule, and any subsequent rule:
(1) The People's Republic of China, including the Hong Kong Special Administrative Region (China);
(2) Republic of Cuba (Cuba);
(3) Islamic Republic of Iran (Iran);
(4) Democratic People's Republic of Korea (North Korea);
(5) Russian Federation (Russia); and
(6) Venezuelan politician Nicolás Maduro (Maduro Regime).
(b) The Secretary's determination of foreign adversaries is solely for the purposes of the Executive Order, this rule, and any subsequent rule promulgated pursuant to the Executive Order. Pursuant to the Secretary's discretion, the list of foreign adversaries will be revised as determined to be necessary. Such revisions will be effective immediately upon publication in the FEDERAL REGISTER without prior notice or opportunity for public comment.
(c) The Secretary's determination is based on multiple sources, including:
(1) National Security Strategy of the United States;
(2) The Director of National Intelligence's 2016–2019 Worldwide Threat Assessments of the U.S. Intelligence Community;
(3) The 2018 National Cyber Strategy of the United States of America; and
(4) Reports and assessments from the U.S. Intelligence Community, the U.S. Departments of Justice, State and Homeland Security, and other relevant sources.
(d) (d) The Secretary will periodically review this list in consultation with appropriate agency heads and

may add to, subtract from, supplement, or otherwise amend this list. Any amendment to this list will apply to any ICTS Transaction that is initiated, pending, or completed on or after the date that the list is amended.

EFFECTIVE DATE NOTE: At 89 FR 96893, Dec. 6, 2024, §791.4 was amended by revising paragraphs (a)(1), (c) introductory text, (c)(2), (c)(3), and (d), and by removing the second parenthetical ''(d)'' from 791.4(d), effective Feb. 4, 2025. For the convenience of the user, the revised text is set forth as follows:

§ 791.4 Determination of foreign adversaries.

(a) * * *

(1) The People's Republic of China, including the Hong Kong Special Administrative Region and the Macau Special Administrative Region (China);

* * * * *

(c) The Secretary's determination is based on multiple sources, including but not limited to:

* * * * *

(2) The Director of National Intelligence's Worldwide Threat Assessments of the U.S. Intelligence Community;

(3) The National Cyber Strategy of the United States of America; and

* * * * *

(d) The Secretary will periodically review this list in consultation with appropriate agency heads and may add to, subtract from, supplement, or otherwise amend this list. Any amendment to this list will apply to any ICTS Transaction that is initiated, pending, or completed on or after the date that the list is amended.

§ 791.5 Effect on other laws.

Nothing in this part shall be construed as altering or affecting any other authority, process, regulation, investigation, enforcement measure, or review provided by or established under any other provision of Federal law, including prohibitions under the National Defense Authorization Act of 2019, the Federal Acquisition Regulations, or IEEPA, or any other authority of the President or the Congress under the Constitution of the United States.

§ 791.6 Amendment, modification, or revocation.

Except as otherwise provided by law, any determinations, prohibitions, or decisions issued under this part may be amended, modified, or revoked, in whole or in part, at any time.

§ 791.7 Public disclosure of records.

Public requests for agency records related to this part will be processed in accordance with the Department of Commerce's Freedom of Information Act regulations, 15 CFR part 4, or other applicable law and regulation.

Subpart B—Review of ICTS Transactions

§ 791.100 General.

In implementing this part, the Secretary of Commerce may:

(a) Consider any and all relevant information held by, or otherwise made available to, the Federal Government that is not otherwise restricted by law for use for this purpose, including:

(1) Publicly available information;

(2) Confidential business information, as defined in 19 CFR 201.6, or proprietary information;

(3) Classified National Security Information, as defined in Executive Order 13526 (December 29, 2009) and its predecessor executive orders, and Controlled Unclassified Information, as defined in Executive Order 13556 (November 4, 2010);

(4) Information obtained from state, local, tribal, or foreign governments or authorities;

(5) Information obtained from parties to a transaction, including records related to such transaction that any party uses, processes, or retains, or would be expected to use, process, or retain, in their ordinary course of business for such a transaction;

(6) Information obtained through the authority granted under sections 2(a) and (c) of the Executive Order and IEEPA, as set forth in U.S.C. 7.101;

(7) Information provided by any other U.S. Government national security body, in each case only to the extent

necessary for national security purposes, and subject to applicable confidentiality and classification requirements, including the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector and the Federal Acquisitions Security Council and its designated information-sharing bodies; and

(8) Information provided by any other U.S. Government agency, department, or other regulatory body, including the Federal Communications Commission, Department of Homeland Security, and Department of Justice;

(b) Consolidate the review of any ICTS Transactions with other transactions already under review where the Secretary determines that the transactions raise the same or similar issues, or that are otherwise properly consolidated;

(c) In consultation with the appropriate agency heads, in determining whether an ICTS Transaction involves ICTS designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, consider the following:

(1) Whether the person or its suppliers have headquarters, research, development, manufacturing, test, distribution, or service facilities, or other operations in a foreign country, including one controlled by, or subject to the jurisdiction of, a foreign adversary;

(2) Ties between the person—including its officers, directors or similar officials, employees, consultants, or contractors—and a foreign adversary;

(3) Laws and regulations of any foreign adversary in which the person is headquartered or conducts operations, including research and development, manufacturing, packaging, and distribution; and

(4) Any other criteria that the Secretary deems appropriate;

(d) In consultation with the appropriate agency heads, in determining whether an ICTS Transaction poses an undue or unacceptable risk, consider the following:

(1) Threat assessments and reports prepared by the Director of National Intelligence pursuant to section 5(a) of the Executive Order;

(2) Removal or exclusion orders issued by the Secretary of Homeland Security, the Secretary of Defense, or the Director of National Intelligence (or their designee) pursuant to recommendations of the Federal Acquisition Security Council, under 41 U.S.C. 1323;

(3) Relevant provisions of the Defense Federal Acquisition Regulation (48 CFR ch. 2) and the Federal Acquisition Regulation (48 CFR ch. 1), and their respective supplements;

(4) The written assessment produced pursuant to section 5(b) of the Executive Order, as well as the entities, hardware, software, and services that present vulnerabilities in the United States as determined by the Secretary of Homeland Security pursuant to that section;

(5) Actual and potential threats to execution of a ''National Critical Function'' identified by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency;

(6) The nature, degree, and likelihood of consequence to the United States public and private sectors that could occur if ICTS vulnerabilities were to be exploited; and

(7) Any other source or information that the Secretary deems appropriate; and

(e) In the event the Secretary finds that unusual and extraordinary harm to the national security of the United States is likely to occur if all of the procedures specified herein are followed, the Secretary may deviate from these procedures in a manner tailored to protect against that harm.

EFFECTIVE DATE NOTE: At 89 FR 96893, Dec. 6, 2024, §791.100 was amended by revising paragraph (a) introductory text, (a)(6), (7), (8), and (9), paragraph (c) introductory text, paragraph (d) introductory text, (d)(5), and (e), effective Feb. 4, 2025. For the convenience of the user, the revised text is set forth as follows:

§ 791.100 General.

* * * * *

(a) Consider any and all relevant information held by, or otherwise made available to,

the Federal Government that is not otherwise restricted by law for use for this purpose, including:

* * * * *

(6) Information obtained through the authority granted under sections 2(a) and (c) of the Executive Order and IEEPA, as set forth in § 791.101 of this part;

(7) Information provided by any other U.S. Government national security body, in each case only to the extent necessary for national security purposes, and subject to applicable confidentiality and classification requirements, including the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector and the Federal Acquisitions Security Council and its designated information-sharing bodies;

(8) Information or referrals provided by any other U.S. Government agency, department, or other regulatory body; and

(9) Information provided voluntarily by private industry.

* * * * *

(c) Determine, in consultation with the appropriate agency heads, whether an ICTS Transaction involves ICTS designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, and in making a determination, the Department may consider the following:

* * * * *

(d) Determine, in consultation with the appropriate agency heads, whether a Covered ICTS Transaction poses an undue or unacceptable risk, considering the following:

* * * * *

(5) Actual or potential threats to execution of a ''National Critical Function'' identified by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency;

* * * * *

(e) In the event the Secretary finds that unusual and extraordinary harm to the national security of the United States is likely to occur if all of the procedures specified herein are followed, deviate from these procedures in a manner tailored to protect against that harm.

§ 791.101 Information to be furnished on demand.

(a) Pursuant to the authority granted to the Secretary under sections 2(a), 2(b), and 2(c) of the Executive Order and IEEPA, persons involved in an ICTS Transaction may be required to furnish under oath, in the form of reports or otherwise, at any time as may be required by the Secretary, complete information relative to any act or transaction, subject to the provisions of this part. The Secretary may require that such reports include the production of any books, contracts, letters, papers, or other hard copy or electronic documents relating to any such act, transaction, or property, in the custody or control of the persons required to make such reports. Reports with respect to transactions may be required either before, during, or after such transactions. The Secretary may, through any person or agency, conduct investigations, hold hearings, administer oaths, examine witnesses, receive evidence, take depositions, and require by subpoena the attendance and testimony of witnesses and the production of any books, contracts, letters, papers, and other hard copy or documents relating to any matter under investigation, regardless of whether any report has been required or filed in connection therewith.

(b) For purposes of paragraph (a) of this section, the term ''document'' includes any written, recorded, or graphic matter or other means of preserving thought or expression (including in electronic format), and all tangible things stored in any medium from which information can be processed, transcribed, or obtained directly or indirectly, including correspondence, memoranda, notes, messages, contemporaneous communications such as text and instant messages, letters, emails, spreadsheets, metadata, contracts, bulletins, diaries, chronological data, minutes, books, reports, examinations, charts, ledgers, books of account, invoices, air waybills, bills of lading, worksheets, receipts, printouts, papers, schedules, affidavits, presentations, transcripts, surveys, graphic representations of any kind, drawings,

photographs, graphs, video or sound recordings, and motion pictures or other film.

(c) Persons providing documents to the Secretary pursuant to this section must produce documents in a format useable to the Department of Commerce, which may be detailed in the request for documents or otherwise agreed to by the parties.

EFFECTIVE DATE NOTE: At 89 FR 96894, Dec. 6, 2024, §791.101 was amended by revising paragraphs (a) and (b), effective Feb. 4, 2025. For the convenience of the user, the revised text is set forth as follows:

§ 791.101 Information to be furnished on demand.

(a) Pursuant to the authority granted to the Secretary under sections 2(a), 2(b), and 2(c) of the Executive Order and IEEPA, the Secretary may require any person to furnish under oath, in the form of reports or otherwise, at any time as may be required by the Secretary, complete information relative to any act or transaction, subject to the provisions of this part. The Secretary may require that such reports include the production of any books, contracts, letters, papers, or other hard copy or electronic documents relating to any such act, transaction, or property, in the custody or control of the persons required to make such reports. Reports with respect to transactions may be required from before, during, or after such transactions. The Secretary may, through any person or agency, conduct investigations, hold hearings, administer oaths, examine witnesses, receive evidence, take depositions, and require by subpoena the attendance and testimony of witnesses and the production of any books, contracts, letters, papers, and other hard copy or documents relating to any matter under investigation, regardless of whether any report has been required or filed in connection therewith.

(b) For purposes of paragraph (a) of this section, the term ''document'' includes any written, recorded, or graphic matter or other means of preserving thought or expression (including in electronic format), and all tangible things stored in any medium from which information can be processed, transcribed, or obtained directly or indirectly, including correspondence, memoranda, notes, messages, contemporaneous communications such as text and instant messages, letters, emails, spreadsheets, metadata, contracts, bulletins, diaries, chronological data, minutes, books, reports, examinations, charts, ledgers, books of account, invoices, air waybills, bills of lading, worksheets, receipts, printouts, papers, schedules, affidavits, presentations, transcripts, surveys, graphic representations of any kind, drawings, photographs, images, graphs, video or sound recordings, and motion pictures or other media such as film.

* * * * *

§ 791.102 Confidentiality of information.

(a) Information or documentary materials, not otherwise publicly or commercially available, submitted or filed with the Secretary under this part will not be released publicly except to the extent required by law.

(b) The Secretary may disclose information or documentary materials that are not otherwise publicly or commercially available and referenced in paragraph (a) in the following circumstances:

(1) Pursuant to any administrative or judicial proceeding;

(2) Pursuant to an act of Congress;

(3) Pursuant to a request from any duly authorized committee or subcommittee of Congress;

(4) Pursuant to any domestic governmental entity, or to any foreign governmental entity of a United States ally or partner, information or documentary materials, not otherwise publicly or commercially available and important to the national security analysis or actions of the Secretary, but only to the extent necessary for national security purposes, and subject to appropriate confidentiality and classification requirements;

(5) Where the parties or a party to a transaction have consented, the information or documentary material that are not otherwise publicly or commercially available may be disclosed to third parties; and

(6) Any other purpose authorized by law.

(c) This section shall continue to apply with respect to information and documentary materials that are not otherwise publicly or commercially available and submitted to or obtained by the Secretary even after the Secretary issues a final determination pursuant to §791.109.

(d) The provisions of 18 U.S.C. 1905, relating to fines and imprisonment and other penalties, shall apply with respect to the disclosure of information

or documentary material provided to the Secretary under these regulations.

[86 FR 4923, Jan. 19, 2021. Redesignated and amended at 89 FR 58265, July 18, 2024]

EFFECTIVE DATE NOTE: At 89 FR 96894, Dec. 6, 2024, § 791.102 was amended by revising the introductory text of paragraph (b), (b)(4) through (6), and adding (b)(7), effective Feb. 4, 2025. For the convenience of the user, the added and revised text is set forth as follows:

§ 791.102 Confidentiality of information.

* * * * *

(b) The Secretary may, subject to appropriate confidentiality and classification requirements, disclose information or documentary materials that are not otherwise publicly or commercially available and referenced in paragraph (a) of this section in the following circumstances:

* * * * *

(4) Pursuant to a request from any domestic governmental entity or any foreign governmental entity of a United States ally or partner, but only to the extent necessary for national security purposes;

(5) Where the parties or a party to a transaction have consented, the information or documentary material that is not otherwise publicly or commercially available may be disclosed to third parties;

(6) Where the Secretary has determined that at least one Covered ICTS Transaction related to the information or documents presents an undue or unacceptable risk, and disclosure to the public or to affected third parties is necessary to prevent or significantly reduce imminent harm to U.S. national security, or the security and safety of United States persons; and

(7) Any other purpose authorized by law.

* * * * *

§ 791.103 Initial review of ICTS Transactions.

(a) Upon receipt of any information identified in § 791.100(a), upon written request of an appropriate agency head, or at the Secretary's discretion, the Secretary may consider any referral for review of a transaction (referral).

(b) In considering a referral pursuant to paragraph (a), the Secretary shall assess whether the referral falls within the scope of § 791.3(a) and involves ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, and determine whether to:

(1) Accept the referral and commence an initial review of the transaction;

(2) Request additional information, as identified in § 791.100(a), from the referring entity regarding the referral; or

(3) Reject the referral.

(c) Upon accepting a referral pursuant to paragraph (b) of this section, the Secretary shall conduct an initial review of the ICTS Transaction and assess whether the ICTS Transaction poses an undue or unacceptable risk, which may be determined by evaluating the following criteria:

(1) The nature and characteristics of the information and communications technology or services at issue in the ICTS Transaction, including technical capabilities, applications, and market share considerations;

(2) The nature and degree of the ownership, control, direction, or jurisdiction exercised by the foreign adversary over the design, development, manufacture, or supply at issue in the ICTS Transaction;

(3) The statements and actions of the foreign adversary at issue in the ICTS Transaction;

(4) The statements and actions of the persons involved in the design, development, manufacture, or supply at issue in the ICTS Transaction;

(5) The statements and actions of the parties to the ICTS Transaction;

(6) Whether the ICTS Transaction poses a discrete or persistent threat;

(7) The nature of the vulnerability implicated by the ICTS Transaction;

(8) Whether there is an ability to otherwise mitigate the risks posed by the ICTS Transaction;

(9) The severity of the harm posed by the ICTS Transaction on at least one of the following:

(i) Health, safety, and security;

(ii) Critical infrastructure;

(iii) Sensitive data;

(iv) The economy;

(v) Foreign policy;

(vi) The natural environment; and

(vii) National Essential Functions (as defined by Federal Continuity Directive-2 (FCD–2)); and

(10) The likelihood that the ICTS Transaction will in fact cause threatened harm.

(d) For ICTS Transactions involving connected software applications that are accepted for review, the Secretary's assessment of whether the ICTS Transaction poses an undue or unacceptable risk may be determined by evaluating the criteria in paragraph (c) as well as the following additional criteria:

(1) Ownership, control, or management by persons that support a foreign adversary's military, intelligence, or proliferation activities;

(2) Use of the connected software application to conduct surveillance that enables espionage, including through a foreign adversary's access to sensitive or confidential government or business information, or sensitive personal data;

(3) Ownership, control, or management of connected software applications by persons subject to the jurisdiction or direction of a foreign adversary;

(4) Ownership, control, or management of connected software applications by persons involved in malicious cyber activities;

(5) Whether there is regular, thorough, and reliable third-party auditing of connected software applications;

(6) The scope and sensitivity of the data collected;

(7) The number and sensitivity of the users with access to the connected software application; and

(8) The extent to which identified risks have been or can be mitigated using measures that can be verified by independent third parties.

(e) If the Secretary finds that an ICTS Transaction does not meet the criteria of paragraph (b) of this section:

(1) The transaction shall no longer be under review; and

(2) Future review of the transaction shall not be precluded, where additional information becomes available to the Secretary.

[86 FR 4923, Jan. 19, 2021, as amended at 88 FR 39358, June 16, 2023. Redesignated and amended at 89 FR 58265, July 18, 2024]

EFFECTIVE DATE NOTE: At 89 FR 96894, Dec. 6, 2024, § 791.103 was revised, effective Feb. 4, 2025. For the convenience of the user, the revised text is set forth as follows:

§ 791.103 Review of ICTS Transactions.

(a) After considering materials described in § 791.100(a), the Secretary may, at the Secretary's discretion, initiate a review of an ICTS Transaction.

(b) As part of the review, the Secretary will assess whether the transaction:

(1) Constitutes a Covered ICTS Transaction, as described in § 791.3;

(2) Involves ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as described in § 791.100(c); and

(3) Poses an undue or unacceptable risk as described in §§ 791.100(d) and 791.103(c).

(c) In assessing whether the Covered ICTS Transaction poses an undue or unacceptable risk, the Secretary may evaluate, among other relevant factors, the following criteria:

(1) The nature and characteristics of the ICTS at issue in the Covered ICTS Transaction, including technical capabilities, applications, and market share considerations;

(2) The nature and degree of the ownership, control, direction, or jurisdiction exercised by the foreign adversary or foreign adversary persons over the design, development, manufacture, or supply at issue in the Covered ICTS Transaction, to include:

(i) The ownership, control, or management by persons that support a foreign adversary's military, intelligence, or proliferation activities; and

(ii) The ownership, control, or management by persons involved in malicious cyber-enabled activities;

(3) The statements and actions of the foreign adversary at issue in the Covered ICTS Transaction;

(4) The statements and actions of the persons involved in the design, development, manufacture, or supply of the ICTS at issue in the Covered ICTS Transaction;

(5) The statements and actions of the parties to the Covered ICTS Transaction;

(6) Whether the Covered ICTS Transaction poses a discrete or persistent threat;

(7) The nature and characteristics of the customer base, business relationships, and operating locations of the parties to the Covered ICTS Transaction;

(8) Whether there is an ability to otherwise mitigate the risks posed by the Covered ICTS Transaction;

(9) The severity of the harm posed by the Covered ICTS Transaction on at least one of the following:

(i) Health, safety, and security;

(ii) Critical infrastructure;

(iii) Sensitive data;

(iv) The economy;

(v) Foreign policy;

(vi) The natural environment; and

(vii) National Essential Functions (as defined by Federal Continuity Directive-2 (FCD–2));

(10) The likelihood that the Covered ICTS Transaction will result in the threatened harm; and

(11) For ICTS Transactions involving connected software applications:

(i) the number and sensitivity of the users with access to the connected software application;

(ii) the scope and sensitivity of any data collected by the connected software application;

(iii) any use of the connected software application to conduct surveillance that enables espionage, including through a foreign adversary's access to sensitive or confidential government or business information, or sensitive personal data;

(iv) whether there is regular, thorough, and reliable third-party auditing of the connected software application; and

(v) the extent to which identified risks have been or can be mitigated using measures that can be verified by independent third parties.

(d) If the Secretary finds that an ICTS Transaction does not meet the criteria of paragraph (b) of this section:

(1) The transaction shall no longer be under review; and

(2) Future review of the transaction shall not be precluded, where additional information becomes available to the Secretary.

§ 791.104 First interagency consultation.

Upon finding that an ICTS Transaction likely meets the criteria set forth in § 791.103(c) during the initial review under § 791.103, the Secretary shall notify the appropriate agency heads and, in consultation with them, shall determine whether the ICTS Transaction meets the criteria set forth in § 791.103(c).

[86 FR 4923, Jan. 19, 2021. Redesignated and amended at 89 FR 58265, July 18, 2024]

EFFECTIVE DATE NOTE: At 89 FR 96895, Dec. 6, 2024, § 791.104 was revised, effective Feb. 4, 2025. For the convenience of the user, the revised text is set forth as follows:

§ 791.104 First interagency notification.

(a) If the Secretary assesses that an ICTS Transaction meets the criteria under § 791.103(b), the Secretary shall memorialize that assessment, provide the assessment to the appropriate agency heads, and offer the appropriate agency heads twenty-one (21) days to comment in writing on the Secretary's assessment.

(b) If the Secretary does not receive written comments on the assessment from an appropriate agency head within twenty-one (21) days of notification, the Secretary may presume that agency has no comments.

(c) The Secretary may, at the Secretary's discretion, modify or revise the assessment based on comments received from the appropriate agency heads. The Secretary retains discretion to make an Initial Determination, as provided in § 791.105, regardless of the comments received.

§ 791.105 Initial determination.

(a) If, after the consultation required by § 791.104, the Secretary determines that the ICTS Transaction does not meet the criteria set forth in § 791.103(c):

(1) The transaction shall no longer be under review; and

(2) Future review of the transaction shall not be precluded, where additional information becomes available to the Secretary.

(b) If, after the consultation required by § 791.104, the Secretary determines that the ICTS Transaction meets the criteria set forth in § 791.103(c), the Secretary shall:

(1) Make an initial written determination, which shall be dated and signed by the Secretary, that:

(i) Explains why the ICTS Transaction meets the criteria set forth in § 791.103(c); and

(ii) Sets forth whether the Secretary has initially determined to prohibit the ICTS Transaction or to propose mitigation measures, by which the ICTS Transaction may be permitted; and

(2) Notify the parties to the ICTS Transaction either through publication in the FEDERAL REGISTER or by serving a copy of the initial determination on the parties via registered U.S. mail, facsimile, and electronic transmission, or third-party commercial carrier, to an addressee's last known address or by personal delivery.

(c) Notwithstanding the fact that the initial determination to prohibit or propose mitigation measures on an ICTS Transaction may, in whole or in part, rely upon classified national security information, or sensitive but unclassified information, the initial determination will contain no classified national security information, nor reference thereto, and, at the Secretary's discretion, may not contain sensitive but unclassified information.

[86 FR 4923, Jan. 19, 2021. Redesignated and amended at 89 FR 58265, July 18, 2024]

EFFECTIVE DATE NOTE: At 89 FR 96895, Dec. 6, 2024, § 791.105 was revised, effective Feb. 4, 2025. For the convenience of the user, the revised text is set forth as follows:

§ 791.105 Initial Determination.

(a) If, after notifying the appropriate agency heads as required by § 791.104 and considering any comments received, the Secretary determines that the Covered ICTS Transaction does not meet the criteria set forth in § 791.103:

(1) The transaction shall no longer be under review; and

(2) Future review of the transaction shall not be precluded, where additional information becomes available to the Secretary.

(b) If, after notifying the appropriate agency heads as required by § 791.104 and considering any comments received, the Secretary determines that the Covered ICTS Transaction meets the criteria set forth in § 791.103, the Secretary shall:

(1) Make a written Initial Determination, which shall be dated and signed by the Secretary, that:

(i) Explains why the ICTS Transaction meets the criteria set forth in § 791.103;

(ii) Sets forth whether the Secretary proposes to prohibit the Covered ICTS Transaction or to impose mitigation measures, by which the Covered ICTS Transaction may be permitted; and

(iii) Provides information regarding the factual basis supporting the decision that is set forth pursuant to subparagraph (ii) above;

(2) Provide at least twenty-one (21) calendar days' notice to the appropriate agency heads of the proposed Initial Determination prior to taking any action under 791.105(b)(3); and

(3) Notify a party or the parties to the Covered ICTS Transaction by:

(i) Serving a copy of the Initial Determination to the identified parties to the Covered ICTS Transaction when the Covered ICTS Transaction under review consists of a single transaction or a set of transactions between a limited number of parties (for example, the sale of ICTS by a company with a foreign nexus to an identified United States person); or

(ii) Serving a copy of the Initial Determination to the person whose ICTS the Secretary determines constitutes the Covered ICTS Transactions under review when the number of U.S. parties or users acquiring, importing, transferring, installing, dealing in, or using the ICTS is unknown or unidentified, or notice to such U.S. parties or users is not feasible or appropriate (for example, when individual consumers purchase the ICTS through an online service or at a retail location).

(c) Notwithstanding the fact that the Initial Determination to prohibit or propose mitigation measures on an ICTS Transaction may, in whole or in part, rely upon classified national security information, or sensitive but unclassified information, the Initial Determination will contain no classified national security information, nor reference thereto, and, at the Secretary's discretion, may not contain controlled unclassified information.

(d) Notwithstanding paragraph (b)(3) of this section, the Secretary may, at the Secretary's discretion, determine to publish any notice of an Initial Determination in the FEDERAL REGISTER.

§ 791.106 Recordkeeping requirement.

Upon notification that an ICTS Transaction is under review or that an initial determination concerning an ICTS Transaction has been made, a notified person must immediately take steps to retain any and all records relating to such transaction.

EFFECTIVE DATE NOTE: At 89 FR 96895, Dec. 6, 2024, § 791.106 was revised, effective Feb. 4, 2025. For the convenience of the user, the revised text is set forth as follows:

§ 791.106 Recordkeeping requirement.

Upon notification that an ICTS Transaction is under review, such as, though not limited to, through a demand for information or documents related to an ICTS Transaction under § 791.101 or a notification that an Initial Determination concerning an ICTS Transaction has been made, a notified person must immediately take steps to retain any and all records relating to such Transaction and must retain such records for no less than ten (10) years following a Final Determination made under § 791.109 or as otherwise indicated in the Final Determination. If a notified person receives no notification that an Initial Determination concerning an ICTS Transaction has been made within ten (10) years of notification that an ICTS Transaction is under review, then the recordkeeping obligation will extend for ten (10) years following the initial notification of an ICTS Transaction review unless the notified person is informed otherwise by the Secretary.

§ 791.107 Procedures governing response and mitigation.

Within 30 days of service of the Secretary's notification pursuant to § 791.105, a party to an ICTS Transaction may respond to the Secretary's initial determination or assert that the circumstances resulting in the initial determination no longer apply, and thus seek to have the initial determination rescinded or mitigated pursuant to the following administrative procedures:

(a) A party may submit arguments or evidence that the party believes establishes that insufficient basis exists for the initial determination, including any prohibition of the ICTS Transaction;

(b) A party may propose remedial steps on the party's part, such as corporate reorganization, disgorgement of control of the foreign adversary, engagement of a compliance monitor, or similar steps, which the party believes would negate the basis for the initial determination;

(c) Any submission must be made in writing;

(d) A party responding to the Secretary's initial determination may request a meeting with the Department, and the Department may, at its discretion, agree or decline to conduct such meetings prior to making a final determination pursuant to § 791.109;

(e) This rule creates no right in any person to obtain access to information in the possession of the U.S. Government that was considered in making the initial determination to prohibit the ICTS Transaction, to include classified national security information or sensitive but unclassified information; and

(f) If the Department receives no response from the parties within 30 days after service of the initial determination to the parties, the Secretary may determine to issue a final determination without the need to engage in the consultation process provided in section 791.108.

[86 FR 4923, Jan. 19, 2021. Redesignated and amended at 89 FR 58265, July 18, 2024]

EFFECTIVE DATE NOTE: At 89 FR 96895, Dec. 6, 2024, § 791.107 was amended by revising the introductory text, paragraphs (c), (e), (f), effective Feb. 4, 2025. For the convenience of the user, the revised text is set forth as follows:

§ 791.107 Procedures governing response and mitigation.

Within 30 days of service of the Secretary's Initial Determination pursuant to § 791.105, a party to a transaction may respond to the Initial Determination or assert that the circumstances resulting in the Initial Determination no longer apply, and thus seek to have the Initial Determination rescinded or mitigated pursuant to the following administrative procedures:

* * * * *

(c) All submissions under this section must be made in writing.

(1) The Secretary may, for good cause, extend the time to provide a written submission pursuant to this section.

(2) Any extensions granted pursuant to this section shall not exceed thirty (30) days.

(3) A written submission to the Secretary pursuant to this section may not exceed fifty (50) pages without approval from the Secretary prior to the expiration of time for a party's response.

(4) A written submission to the Secretary may include business confidential information. Any business confidential information must be clearly and specifically demarcated. Publicly available information should not be marked business confidential.

* * * * *

(e) This rule creates no right in any person to obtain access to information in the possession of the U.S. Government that was considered in making the Initial Determination, to include classified national security information or sensitive but unclassified information; and

(f) If the Department receives no response from the parties within 30 days after service of the Initial Determination to the parties, the Secretary may issue a Final Determination without the need to engage in the consultation process provided in section 791.108 of this rule.

§ 791.108 Second interagency consultation.

(a) Upon receipt of any submission by a party to an ICTS Transaction under § 791.107, the Secretary shall consider whether and how any information provided—including proposed mitigation measures—affects an initial determination of whether the ICTS Transaction meets the criteria set forth in § 791.103(c).

(b) After considering the effect of any submission by a party to an ICTS Transaction under § 791.107 consistent with paragraph (a) of this section, the Secretary shall consult with and seek the consensus of all appropriate agency heads prior to issuing a final determination as to whether the ICTS Transaction shall be prohibited, not prohibited, or permitted pursuant to the adoption of negotiated mitigation measures.

(c) If consensus is unable to be reached, the Secretary shall notify the President of the Secretary's proposed final determination and any appropriate agency head's opposition thereto.

(d) After receiving direction from the President regarding the Secretary's proposed final determination and any appropriate agency head's opposition thereto, the Secretary shall issue a final determination pursuant to § 791.109.

[86 FR 4923, Jan. 19, 2021. Redesignated and amended at 89 FR 58265, July 18, 2024]

EFFECTIVE DATE NOTE: At 89 FR 96896, Dec. 6, 2024, § 791.108 was revised, effective Feb. 4, 2025. For the convenience of the user, the revised text is set forth as follows:

§ 791.108 Interagency consultation on the Final Determination.

(a) Upon receipt of any submission by a party to a transaction under § 791.107, the Secretary shall consider whether and how the information provided—including proposed mitigation measures—affects an Initial Determination.

(b) After considering the effect of any submission by a party to a transaction under § 791.107 consistent with paragraph (a) of this section, the Secretary shall provide notice in writing of the proposed Final Determination and consult with and seek concurrence from all appropriate agency heads prior to issuing a Final Determination as to whether the Covered ICTS Transaction shall be prohibited, not prohibited, or permitted pursuant to the adoption of negotiated mitigation measures.

(c) If the appropriate agency heads under paragraph (b) of this section concur, the Secretary shall issue a Final Determination pursuant to § 791.109. If an appropriate agency head provides no response within fourteen (14) days of the agency receiving the notice in writing of the proposed Final Determination, the Secretary may presume concurrence. If an agency objects to the Final Determination, such objection must be submitted by the agency's Deputy Secretary or equivalent or higher level within the 14 days.

§ 791.109 Final determination.

(a) For each transaction for which the Secretary issues an initial determination that an ICTS Transaction is prohibited, the Secretary shall issue a final determination as to whether the ICTS Transaction is:

(1) Prohibited;

(2) Not prohibited; or

(3) Permitted, at the Secretary's discretion, pursuant to the adoption of negotiated mitigation measures.

(b) Unless the Secretary determines in writing that additional time is necessary, the Secretary shall issue the final determination within 180 days of accepting a referral and commencing the initial review of the ICTS Transaction pursuant to § 791.103.

(c) If the Secretary determines that an ICTS Transaction is prohibited, the Secretary shall have the discretion to direct the least restrictive means necessary to tailor the prohibition to address the undue or unacceptable risk posed by the ICTS Transaction.

(d) The final determination shall:

(1) Be written, signed, and dated;

(2) Describe the Secretary's determination;

(3) Be unclassified and contain no reference to classified national security information;

(4) Consider and address any information received from a party to the ICTS Transaction;

(5) Direct, if applicable, the timing and manner of the cessation of the ICTS Transaction;

(6) Explain, if applicable, that a final determination that the ICTS Transaction is not prohibited does not preclude the future review of transactions related in any way to the ICTS Transaction;

(7) Include, if applicable, a description of the mitigation measures agreed upon by the party or parties to the ICTS Transaction and the Secretary; and

(8) State the penalties a party will face if it fails to comply fully with any mitigation agreement or direction, including violations of IEEPA, or other violations of law.

(e) The written, signed, and dated final determination shall be sent to:

(1) The parties to the ICTS Transaction via registered U.S. mail and electronic mail; and

(2) The appropriate agency heads.

(f) The results of final written determinations to prohibit an ICTS Transaction shall be published in the FEDERAL REGISTER. The publication shall

omit any confidential business information.

[86 FR 4923, Jan. 19, 2021. Redesignated and amended at 89 FR 58265, July 18, 2024]

EFFECTIVE DATE NOTE: At 89 FR 96896, Dec. 6, 2024, § 791.109 was revised, effective Feb. 4, 2025. For the convenience of the user, the revised text is set forth as follows:

§ 791.109 Final Determination.

(a) For each Covered ICTS Transaction for which the Secretary issues an Initial Determination, the Secretary shall issue a Final Determination as to whether the Covered ICTS Transaction is:

(1) Prohibited;

(2) Not prohibited; or

(3) Permitted, at the Secretary's discretion, pursuant to the adoption of mitigation measures.

(b) Unless the Secretary, at the Secretary's sole discretion, determines in writing that additional time is necessary, the Secretary shall issue the Final Determination within 180 days of serving the Initial Determination pursuant to § 791.105(b)(3).

(c) If the Secretary determines that a Covered ICTS Transaction is prohibited, the Secretary shall direct the means that the Secretary assesses to be necessary to address the undue or unacceptable risk posed by the Covered ICTS Transaction.

(d) The Final Determination shall:

(1) Be written, signed, and dated;

(2) Describe the Secretary's determination;

(3) Be unclassified and contain no reference to classified national security information;

(4) Consider and address any information received from a party or parties to the transaction;

(5) Direct, if applicable, the timing and manner of the cessation of the Covered ICTS Transaction;

(6) Explain, if applicable, that a Final Determination that the Covered ICTS Transaction is not prohibited does not preclude the future review of transactions related in any way to the Covered ICTS Transaction;

(7) Include, if applicable, a description of the mitigation measures agreed upon by the party or parties to the transaction and the Secretary;

(8) State the penalties a party will face if it fails to comply fully with any mitigation agreement or direction, including violations of IEEPA, or other violations of law; and

(9) Include, if applicable, how the Department may transition a mitigation agreement to a prohibition should a party or parties fail to comply with any mitigation agreement or obligations, or violate IEEPA or other law.

(e) The written, signed, and dated Final Determination shall be sent to:

(1) The party or parties to the transaction that are identified in the Final Determination via registered U.S. mail and electronic mail; and

(2) The appropriate agency heads.

(f) The Secretary shall publish a notice of any Final Determination to prohibit an ICTS Transaction in the FEDERAL REGISTER. The Secretary shall also publish a notice of Final Determination for any ICTS Transaction for which the Secretary published a notice of an Initial Determination. The Secretary may publish a notice of a Final Determination to mitigate an ICTS Transaction in the FEDERAL REGISTER. Any notice of a Final Determination that is published in the FEDERAL REGISTER shall omit any confidential business information.

§ 791.110 Classified national security information.

In any review of a determination made under this part, if the determination was based on classified national security information, such information may be submitted to the reviewing court *ex parte* and *in camera*. This section does not confer or imply any right to review in any tribunal, judicial or otherwise.

Subpart C—Enforcement

§ 791.200 Penalties.

(a) Maximum penalties.

(1) *Civil penalty*. A civil penalty not to exceed the amount set forth in Section 206 of IEEPA, 50 U.S.C. 1705, may be imposed on any person who violates, attempts to violate, conspires to violate, or causes any knowing violation of any final determination or direction issued pursuant to this part, including any violation of a mitigation agreement issued or other condition imposed under this part. IEEPA provides for a maximum civil penalty not to exceed the greater of $250,000, subject to inflationary adjustment, or an amount that is twice the amount of the transaction that is the basis of the violation with respect to which the penalty is imposed.

(2) *Criminal penalty*. A person who willfully commits, willfully attempts to commit, or willfully conspires to commit, or aids and abets in the commission of a violation of any final determination, direction, or mitigation agreement shall, upon conviction of a violation of IEEPA, be fined not more than $1,000,000, or if a natural person,