NAVAID. Interested parties were invited to participate in this rulemaking effort by submitting written comments on the proposal. No comments were received.

Differences From the NPRM

Subsequent to the NPRM, the FAA published a final rule for Docket No. FAA–2023–2483 in the **Federal Register** (89 FR 48504; June 7, 2024), amending VOR Federal Airway V–216 by removing the airway segment between the Lamoni VOR/Distance Measuring Equipment (VOR/DME) and the Iowa City, IA, VOR/DME. That airway amendment, effective September 5, 2024, is included in this rule.

Additionally, subsequent to the NPRM, the FAA published a final rule for Docket No. FAA–2023–2466 in the **Federal Register** (89 FR 48506; June 7, 2024), revoking VOR Federal Airway V–380 effective September 5, 2024. As a result, VOR Federal Airway V–380 is removed from this docket action.

Incorporation by Reference

VOR Federal Airways are published in paragraph 6010(a) of FAA Order JO 7400.11, Airspace Designations and Reporting Points, which is incorporated by reference in 14 CFR 71.1 on an annual basis. This document amends the current version of that order, FAA Order JO 7400.11J, dated July 31, 2024, and effective September 15, 2024. FAA Order JO 7400.11J is publicly available as listed in the **ADDRESSES** section of this document. These amendments will be published in the next update to FAA Order JO 7400.11.

FAA Order JO 7400.11J lists Class A, B, C, D, and E airspace areas, air traffic service routes, and reporting points.

The Rule

This action amends 14 CFR part 71 by amending VOR Federal Airway V–216 and revoking VOR Federal Airways V–549 and V–551. The FAA is taking this action due to the planned decommissioning of the VOR portion of the Mankato, KS, VORTAC. The airway actions are described below.

V–216: Prior to this final rule, V–216 extended between the Lamar, IA, VOR/DME and the Mankato, KS, VORTAC; and between the Iowa City, IA, VOR/DME and the Janesville, WI, VOR/DME. The airway segment between the Hill City, KS, VORTAC and the Mankato VORTAC is removed. As amended, the airway is changed to now extend between the Lamar VOR/DME and the Hill City VORTAC, and between the Iowa City VOR/DME and the Janesville VOR/DME.

V–549: Prior to the final rule, V–549 extended between the Hays, KS, VORTAC and the Mankato, KS, VORTAC. The airway is removed in its entirety.

V–551: Prior to this final rule, V–551 extended between the Salina, KS, VORTAC and the Mankato, KS, VORTAC. The airway is removed in its entirety.

The NAVAID radials listed in the V–216 description in the regulatory text of this final rule are unchanged and stated in degrees True north.

Regulatory Notices and Analyses

The FAA has determined that this regulation only involves an established body of technical regulations for which frequent and routine amendments are necessary to keep them operationally current. It, therefore: (1) is not a ''significant regulatory action'' under Executive Order 12866; (2) is not a ''significant rule'' under DOT Regulatory Policies and Procedures (44 FR 11034; February 26, 1979); and (3) does not warrant preparation of a regulatory evaluation as the anticipated impact is so minimal. Since this is a routine matter that only affects air traffic procedures and air navigation, it is certified that this rule, when promulgated, does not have a significant economic impact on a substantial number of small entities under the criteria of the Regulatory Flexibility Act.

Environmental Review

The FAA has determined that this action amending VOR Federal Airway V–216 and revoking VOR Federal Airways V–549 and V–551, due to the planned decommissioning of the VOR portion of the Mankato, KS, VORTAC NAVAID, qualifies for categorical exclusion under the National Environmental Policy Act (42 U.S.C. 4321 *et seq.*) and its implementing regulations at 40 CFR part 1500, and in accordance with FAA Order 1050.1F, Environmental Impacts: Policies and Procedures, paragraph 5–6.5a, which categorically excludes from further environmental impact review rulemaking actions that designate or modify classes of airspace areas, airways, routes, and reporting points (see 14 CFR part 71, Designation of Class A, B, C, D, and E Airspace Areas; Air Traffic Service Routes; and Reporting Points). As such, this action is not expected to result in any potentially significant environmental impacts. In accordance with FAA Order 1050.1F, paragraph 5–2 regarding Extraordinary Circumstances, the FAA has reviewed this action for factors and circumstances in which a normally categorically excluded action may have a significant environmental impact requiring further analysis. The FAA has determined that no extraordinary circumstances exist that warrant preparation of an environmental assessment or environmental impact study.

List of Subjects in 14 CFR Part 71

Airspace, Incorporation by reference, Navigation (air).

The Amendment

In consideration of the foregoing, the Federal Aviation Administration amends 14 CFR part 71 as follows:

PART 71—DESIGNATION OF CLASS A, B, C, D, AND E AIRSPACE AREAS; AIR TRAFFIC SERVICE ROUTES; AND REPORTING POINTS

■ 1. The authority citation for 14 CFR part 71 continues to read as follows:

Authority: 49 U.S.C. 106(f); 40103, 40113, 40120; E.O. 10854, 24 FR 9565, 3 CFR, 1959–1963 Comp., p. 389.

§ 71.1 [Amended]

■ 2. The incorporation by reference in 14 CFR 71.1 of FAA Order JO 7400.11J, Airspace Designations and Reporting Points, dated July 31, 2024, and effective September 15, 2024, is amended as follows:

Paragraph 6010(a) Domestic VOR Federal Airways.

* * * * *

V–216 [Amended]

From Lamar, CO; to Hill City, KS. From Iowa City, IA; INT Iowa City 062° and Janesville, WI, 240° radials; to Janesville.

* * * * *

V–549 [Removed]

* * * * *

V–551 [Removed]

* * * * *

Issued in Washington, DC, on December 3, 2024.

Richard Lee Parks,

Manager (A), Rules and Regulations Group.

[FR Doc. 2024–28576 Filed 12–5–24; 8:45 am]

BILLING CODE 4910–13–P

DEPARTMENT OF COMMERCE

15 CFR Part 791

[Docket No. 241112–0292]

RIN 0605–AA51

Securing the Information and Communications Technology and Services Supply Chain

AGENCY: U.S. Department of Commerce

ACTION: Final rule.

SUMMARY: On January 19, 2021, the Department of Commerce (Department) issued an interim final rule establishing procedures for its review of transactions involving information and communications technology and services (ICTS) designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary that may pose undue or unacceptable risk to the United States or U.S. persons. In the interim final rule, the Department solicited public comments and committed to promulgating a final rule. This final rule responds to public comments on the interim final rule and finalizes the practices guiding review of ICTS Transactions, amending and, in some cases, removing terms or concepts which experience has shown to be unnecessary, inefficient, or ineffective.

DATES: This rule is effective February 4, 2025.

ADDRESSES: Supporting documents:

- The Regulatory Impact Analysis/Final Regulatory Flexibility Analysis (RIA/FRFA) prepared in support of this action is available at *https://www.regulations.gov* at docket number DOC–2019–0005;
- The **Federal Register** notice on the interim final rule (IFR) and public comments on the IFR are available at docket number DOC–2019–0005;
- The National Security Memorandum 22 on Critical Infrastructure Security and Resilience is available at *https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/;*
- The Presidential Policy Directive—Critical Infrastructure Security and Resilience is available at *https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil;*
- The Federal Continuity Directive 2 is available at *https://www.fema.gov/emergency-managers/national-preparedness/continuity/toolkit/resources;*
- The National Security Strategy of the United States is available at *https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf;*
- The Director of National Intelligence's Worldwide Threat Assessments of the U.S. Intelligence Community is available at *https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf;*
- The National Cybersecurity Strategy of the United States is available at: *https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf;*
- The United States Government National Standards Strategy for Critical and Emerging Technology is available at *https://www.whitehouse.gov/wp-content/uploads/2023/05/US-Gov-National-Standards-Strategy-2023.pdf;* and
- The Office of Science and Technology Policy's list of Critical and Emerging Technologies is available at *https://www.whitehouse.gov/wp-content/uploads/2024/02/Critical-and-Emerging-Technologies-List-2024-Update.pdf.*

FOR FURTHER INFORMATION CONTACT: Katelyn Christ, U.S. Department of Commerce, Telephone: (202) 482–3064, email: *ICTsupplychain@doc.gov.* For media inquiries: Katherine Schneider, Office of Congressional and Public Affairs, Bureau of Industry and Security, U.S. Department of Commerce: *OCPA@bis.doc.gov.*

SUPPLEMENTARY INFORMATION:

I. Background

A. Authority

In E.O. 13873, ''Securing the Information and Communications Technology and Services Supply Chain,'' the President delegated to the Secretary of Commerce (Secretary) pursuant to 3 U.S.C. 301, to the extent necessary to implement the order, the authority granted under the International Emergency Economic Powers Act (IEEPA) (50 U.S.C. 1701, *et seq.*), ''to deal with any unusual and extraordinary'' foreign threat to the United States' national security, foreign policy, or economy, if the President declares a national emergency with respect to such threat. 50 U.S.C. 1701(a). In E.O. 13873, the President declared a national emergency with respect to the ''unusual and extraordinary'' foreign threat posed to the ICTS supply chain and has, in accordance with the National Emergencies Act (NEA) (50 U.S.C. 1601, *et seq.*), extended the declaration of this national emergency in each year since E.O. 13873's publication. *See* 85 FR 29321 (May 14, 2020); 86 FR 26339 (May 13, 2021); 87 FR 29645 (May 13, 2022); 88 FR 30635 (May 11, 2023); 89 FR 40353 (May 9, 2024).

Specifically, the President identified the ''unrestricted acquisition or use in the United States of [ICTS] designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries'' as ''an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States'' that ''exists both in the case of individual acquisitions or uses of such technology or services, and when acquisitions or uses of such technologies are considered as a class.'' E.O. 13873; *see also* 50 U.S.C. 1701(a) and (b).

Once the President declares a national emergency, IEEPA empowers the President to, among other acts, investigate, regulate, prevent, or prohibit, any ''acquisition, holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving, any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States.'' 50 U.S.C. 1702(a)(1)(B).

To address the identified risks to national security from ICTS transactions, the President in E.O. 13873 imposed a prohibition on transactions determined by the Secretary, in consultation with relevant agency heads, to involve foreign adversary ICTS and to pose certain risks to U.S. national security, technology, or critical infrastructure. Specifically, to fall within the scope of the prohibition, the Secretary, in consultation with relevant agency heads, must determine that any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology and services (an ICTS Transaction): (1) ''involves [ICTS] designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary,'' defined in E.O. 13873 as ''any foreign government or foreign non-government person 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 (2):

A. ''poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States;''

B. ''poses an undue risk of catastrophic effects on the security or resiliency of United States critical

infrastructure or the digital economy of the United States;'' or

C. ''otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.''

These factors are collectively referred to as ''undue or unacceptable risks.'' Further, E.O. 13873 section 1(b) grants the Secretary the authority to design or negotiate mitigation measures that would allow an otherwise prohibited transaction to proceed.

B. ICTS Transaction Review Regulations

On November 27, 2019, the Department of Commerce (Department) published a proposed rule to implement the terms of E.O. 13873 (84 FR 65316). The proposed rule set forth processes for how: (1) the Secretary would evaluate and assess transactions involving ICTS with a nexus to foreign adversaries to determine whether they pose an undue risk of sabotage to or subversion of the ICTS supply chain, or an unacceptable risk to the national security of the United States or the security and safety of U.S. persons; (2) parties to transactions reviewed by the Secretary could comment on the Secretary's preliminary decisions; and (3) the Secretary would notify parties to transactions of the Secretary's decision regarding ICTS Transactions under review, including whether the Secretary would prohibit the transaction or mitigate the risks posed by the transaction. The proposed rule also provided that the Secretary could act without complying with the proposed procedures where required by national security. Finally, it provided that the Secretary would establish penalties for violations of mitigation agreements, the regulations, or E.O. 13873.

After receiving and reviewing comments to the proposed rule, on January 19, 2021, the Department published an interim final rule titled, ''Securing the Information and Communications Technology and Services Supply Chain,'' (the interim final rule or the IFR; 86 FR 4909). The interim final rule responded to comments to the proposed rule, many of which requested greater specificity about what constitutes ICTS, an ICTS Transaction, or transactions that would be subject to the Department's review.

In response to these and other comments, the IFR defined ''ICTS'' as ''any hardware, software, 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'' (86 FR at 4923). The interim final rule further defined an ''ICTS Transaction'' as ''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 . . . . [t]he term ICTS Transaction includes a class of ICTS Transactions.''

On November 26, 2021, the Department published a notice of proposed rulemaking (NPRM) (86 FR 67379), titled ''Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications,'' seeking comments on amendments to Part 7 incorporating provisions of E.O. 14034, titled ''Protecting Americans' Sensitive Data From Foreign Adversaries'' (86 FR 31423). On June 21, 2023, the Department published a final rule implementing E.O. 14034. That final rule incorporated the term ''connected software applications'' into the regulations at 15 CFR part 7 and added specific factors for the Department to consider when reviewing ICTS Transactions involving connected software applications (88 FR 39353). However, that final rule included only the changes to the regulations that were necessary to implement E.O. 14034 and within the scope of the November 26, 2021, NPRM on connected software applications. The June 21, 2023, final rule for connected software applications was more limited in scope than the January 19, 2021, interim final rule and did not fully respond to public comments on the interim final rule.

On July 18, 2024, the Department published a procedural rule entitled ''Redesignation of Regulations for Securing the Information and Communications Technology and Services Supply Chain'' (89 FR 58263) moving the regulations implementing E.O. 13873 and E.O. 14034 from 15 CFR part 7 to 15 CFR part 791. Consistent with the placement of the Office of Information and Communications Technology and Services (OICTS) within the Bureau of Industry and Security (BIS) on March 15, 2022, following the Consolidated Appropriations Act for Fiscal Year 2022, the action moved OICTS regulations from subtitle A in the CFR, which is generally reserved for Secretarial actions and Department-wide activities and operations, to chapter VII in title 15 of the CFR, where BIS regulations are located. Specifically, this action removed the regulations in title 15, subtitle A, part 7 (under the ''Office of the Secretary of Commerce''), reserving that part, and redesignated them as title 15, subtitle B, chapter VII, subchapter E part 791 (under the ''Bureau of Industry and Security, Department of Commerce''). This procedural rule also established Subchapter E entitled ''Information and Communications Technology and Services Regulations.'' This rule was of a purely procedural nature and did not and does not affect, impact, or alter any of the rules or regulations discussed herein other than moving their location in the CFR. The Department issued the procedural rule to bring the OICTS regulations into the same location in the CFR as the other BIS regulations. The redesignation is reflected in this final rule—any citation to 15 CFR part 7 in the interim final rule is now revised to 15 CFR part 791.

C. Overview of the January 2021 Interim Final Rule

Sections 7.1 through 7.3 of the interim final rule explained the overall purpose of the rule, defined terms used in the regulatory text, and specified the types of ICTS and users of ICTS about which the regulations are primarily concerned, such as those in critical and emerging technologies or critical infrastructure. Sections 7.100 through 7.109 provided procedures for the Department's review of ICTS Transactions to determine whether the transactions pose ''undue'' or ''unacceptable'' risks as those terms are specified in E.O. 13873. Under the procedures set forth in the IFR, the Department could accept a referral of an ICTS Transaction from another agency or could undertake a review of an ICTS Transaction *sua sponte* based on information it possesses or receives. If the Department determined that an ICTS Transaction posed an ''undue'' or ''unacceptable'' risk, the Department could, after consulting with the appropriate agency heads about the potential risks posed by the ICTS Transaction under review, issue an Initial Determination that identifies the risks generally and contains a proposal to prohibit, mitigate, or allow such ICTS Transaction.

The IFR also required that the Initial Determination be followed by a period during which a party to the transaction that is the subject of the Initial Determination could provide the Department with additional information to respond to the Initial Determination or seek to negotiate with the Department to allow the ICTS Transaction, with modifications. Following that period,

and upon reviewing any information provided by parties, and seeking consensus from the appropriate agencies to determine whether to prohibit, mitigate, or allow the ICTS Transaction under review, the Department would issue a Final Determination. Under the IFR, the Final Determination provided information supporting a finding that an ICTS Transaction does or does not pose an undue or unacceptable risk, and assessed any information provided by the party to the transaction under review. Under the IFR, the results of Final Determinations to prohibit an ICTS Transaction were printed in the **Federal Register** without any confidential business information, and they were also provided to the appropriate agency heads as well as the party or parties to the transaction that was the subject of the Final Determination.

Violating orders under IEEPA could result in civil penalties, criminal penalties, or both. Section 7.200 of the IFR captured the authorized penalties for violating a Final Determination order or requirement (in the case of mitigation or prohibition). The penalties could be administrative or criminal in nature, and § 7.200 set out both the standards for when civil or criminal penalties may apply to a violation, as well as the nature and value or duration of any punishment applied for violating a Final Determination order.

II. Overview of Changes Implemented in This Final Rule

After the benefit of two years of implementation experience, the Department is amending some of the provisions of the IFR to improve and make more efficient the ICTS Transaction review process as outlined in 15 CFR part 791. In addition, the Department received and has considered the comments to the IFR and responds to those comments in this final rule.

This final rule specifically adds new definitions and revises existing definitions in § 791.2; amends § 791.3 to remove the requirement that a party must collect sensitive personal data from more than one million U.S. persons to be included in the scope of certain aspects of the regulations, as well as to reorganize and clarify the software, hardware, and other products and services that may be considered for review; adds the Special Administrative Region of Macau as part of the People's Republic of China to the foreign adversary list in § 791.4; clarifies procedures to initiate a review set forth in § 791.103; amends for additional clarity the requirements to notify and consult with appropriate agency heads regarding the Secretary's assessment in §§ 791.104 and 791.108; clarifies who are considered parties to an ICTS Transaction and will be notified of an Initial Determination in § 791.105; clarifies certain procedures for parties' responses to Initial Determinations in § 791.107; lists prohibited activities in § 791.200; and makes clarifying changes to other provisions.

Many of the changes in this final rule are non-substantive in nature. For example, the Department is adding a definition for ''Covered ICTS Transaction'' to clearly distinguish in the rule text between ICTS Transactions generally and ICTS Transactions that meet specific criteria in § 791.3. This change is meant to clarify for the public and parties to ICTS Transactions the process the Department will follow after determining a transaction is a Covered ICTS Transaction.

Although this is a final action, the Department will continue to review its procedures and may consider future rulemakings to further clarify aspects of these regulations, which would involve additional opportunity for stakeholder input.

III. Response to Comments and Discussion of Changes From the Interim Final Rule

During the public comment period for the IFR, which closed on March 22, 2021, the Department received 33 comment letters from a variety of sources, including members of industry, commercial trade groups, and private individuals. All comments received by the end of the comment period are available on the public rulemaking docket for the IFR (see **ADDRESSES** above). Many commenters were generally supportive of the Department's efforts to clarify the scope of the regulations, but commenters believed that the IFR did not completely resolve concerns stakeholders had expressed about the proposed rule. Additionally, commenters expressed concerns about multiple sections of the IFR, including: definitions; the scope of covered ICTS Transactions; foreign adversary determinations; and certain aspects of the Department's process to review ICTS Transactions. The Department has carefully considered all comments and addresses them below. The Department's discussion of comments on the IFR and changes implemented by this final rule are organized in numerical order by section of the rule and comments are addressed in the section to which they pertain. Comments that are either no longer relevant or that are outside the scope of this final rule are summarized at the end of the discussion section below.

Section 791.2—Definitions

The majority of comments the Department received to the IFR requested that the Department develop, amend, or clarify various definitions to provide the public with further clarity about the Department's specific concerns regarding ICTS Transactions and classes of ICTS Transactions and about what the Department intends to regulate. Commenters stated that the definitions in the IFR, which largely were adopted directly from E.O. 13873 without change, were vague and overly broad. In particular, commenters indicated that the terms ''dealing in,'' ''person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary,'' and ''transfer,'' were not defined sufficiently to provide a reasonable understanding of which transactions are subject to prohibition or mitigation under the rule.

Commenters also noted that certain terms used within the definition of ''ICTS Transaction'' were undefined in the IFR. Commenters were concerned that the potential breadth of these terms could discourage U.S. and foreign entities from engaging in ICTS Transactions out of concern that any such transactions could be reviewed and prohibited. Other commenters expressed concerns that leaving undefined the term ''ongoing activities'' in the definition of ICTS Transactions might discourage beneficial activities such as software updates.

As described in detail below, although the Department does not believe it is necessary to provide new definitions for all the terms mentioned by commenters, the Department does agree that certain terms needed additional clarity and, accordingly, is revising and adding definitions for terms in § 791.2. The revised terms are: ''party or parties to a transaction,'' ''Secretary,'' ''United States person,'' ''person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary,'' and ''appropriate agency heads.'' The newly defined terms are: ''covered ICTS transaction,'' ''dealing in,'' and ''importation.'' These include definitions for some of the terms that were used but not defined in the IFR's definition of ICTS Transactions, discussed below. The Department believes that its chosen changes address commenters' concerns and clarify the scope of the definitions in the rule, and does not believe it is necessary to provide definitions for the other terms, for reasons that are discussed below.

(1) Terms within the definition of ''ICTS Transaction.''

The IFR defined an ICTS Transaction as any acquisition, importation, transfer, installation, dealing in, or use of any ICTS, including ongoing activities, such as managed services, data transmission, software updates, repairs, or the platforming or data hosting of applications for consumer download. The IFR also clarified that an ICTS Transaction includes any other transaction designed or intended to evade or circumvent the application of E.O. 13873 and that the term ICTS Transaction includes a class of ICTS Transactions.

This final rule continues to use the definition of ''ICTS Transaction,'' consistent with the IFR, but the Department has clarified this definition by further defining the terms ''dealing in'' and ''importation'' that appear within the definition of ICTS Transaction, as discussed below.

(2) New definition of ''Dealing in'' as used within the definition of ''ICTS Transaction.''

To clarify the definition of ''ICTS Transaction'' this final rule defines ''dealing in,'' as the ''activity of buying, selling, reselling, receiving, licensing, or acquiring ICTS, or otherwise doing or engaging in business involving the conveyance of ICTS.'' This change responds to commenters' concerns that ''dealing in'' is a vague term that could have broad implications for ICTS importers, by emphasizing the provision of ICTS to or into the United States through sales, resales, licensing, or acquisition, rather than other means. Some commenters suggested that the term ''dealing in'' could be defined as ''engaging directly in a financial transaction for the offering, buying, selling, or trading of prohibited ICTS,'' consistent with the Securities and Exchange Act of 1934. However, the Department has not adopted the Securities Exchange Act of 1934 definition of ''dealing in'' because that definition would focus on the financial transaction resulting in a purchase, sale, or trade of ICTS. Because there may be instances in which ICTS is provided as a technology transfer or as a free service, such as some tax services or antivirus detection services, that definition would not capture the full scope of ICTS Transactions of concern in E.O. 13873.

Therefore, the definition of ''dealing in'' in this final rule, which also includes ''receiving,'' ''acquiring,'' or ''licensing'' ICTS, provides more clarity while remaining sufficiently broad to encompass the many ways in which ICTS enters the United States.

(3) New definition of ''Importation'' as used within the definition of ''ICTS Transaction.''

To further clarify the definition of ''ICTS Transaction,'' this final rule adds a definition for the term ''importation'' as ''the process or activity of bringing foreign ICTS to or into the United States, regardless of the means of conveyance, including via electronic transmission.'' This definition is consistent with U.S. import laws, *see, e.g.,* 21 U.S.C. 951, and the generally understood meaning of the term. This change will clarify that the Department interprets the term ''importation'' as used in E.O. 13873 and the defined term ''ICTS Transaction'' to encompass ICTS Transactions in which ICTS is brought to or into the United States and does not include exports, as some commenters had suggested.

The Department notes that, in the execution of its authorities, the Department may, in the context of specific technologies addressed in regulations under this part, further specify the particular meaning of ''importation'' with respect to those technologies. For example, the Department may tailor the scope of ''importation'' for a specific class of ICTS or a specific industry covered by a regulation under this part. In this final rule, the definition of ''importation'' applies broadly to any ICTS, including ICTS transmitted electronically, that is subject to the Department's jurisdiction under E.O. 13873.

(4) Other terms used in the definition of ''ICTS Transaction.''

Some commenters requested that the Department remove the term ''use'' from the definition of ''ICTS Transaction'' or define ''use'' as ''employing ICTS for its intended purpose.'' Other commenters requested that the term ''use'' in ''ICTS Transaction'' apply only to the delivery of goods or services to U.S. consumers and not to research, testing, or standards development. The Department declines to remove ''use'' from the definition of ''ICTS Transaction'' because ''use'' is included in the description of prohibited ICTS Transactions in section 1 of E.O. 13873. Moreover, this final rule does not define ''use'' as suggested by commenters because the Department believes such change would define the term in a way to narrow the term beyond its ordinary meaning. Moreover, the Department does not interpret commenters' proposed limitations of the term ''use'' to be consistent with the objective of E.O. 13873. The Department does not intend to exclude certain uses or misuses of ICTS that present undue or unacceptable risks. Therefore, consistent with E.O. 13873, the Department declines to define ''use'' to avoid limiting the types of transactions that could fall within the definition of ''ICTS Transaction.''

Commenters also noted that the terms ''acquisition,'' ''transfer,'' ''installation,'' and ''ongoing activities'' were not defined in the IFR and could have multiple meanings, resulting in confusion if left undefined. Some of these commenters suggested that the Department either remove these terms from the definition of ICTS Transaction, further elaborate on their meaning, or define these terms in a way that would impact the scope of the regulations. The Department will not remove these terms from the definition of ''ICTS Transaction,'' as removing the terms would be inconsistent with how E.O. 13873 describes ICTS Transactions that could pose undue or unacceptable risk. The Department is also not defining these terms in this final rule. Similar to the Department's decision not to define ''use,'' the Department's interpretation of each of these terms is consistent with their ordinary meanings and their use in E.O. 13873. Defining these terms inconsistently with their ordinary meanings could add unnecessary complexity to the regulatory text. The Department believes that providing definitions for the terms ''acquisition'' and ''installation,'' in particular, is unnecessary. Many comments requesting these definitions focused on the scope of the rule and how the terms ''acquisition'' or ''installation'' could impact the parties that may be subject to a transaction review. In this final rule, the Department is addressing such concerns, to the extent consistent with E.O. 13873, by revising the definition for ''party or parties to a transaction'' and implementing changes in other sections that more directly address the parties that may be subject to an ICTS Transaction review.

(5) Revised definition of ''Party or parties to a transaction.''

As previewed above, the Department is revising the definition of ''party or parties to a transaction.'' The IFR defined this term as 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. The IFR definition excluded 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.

Commenters stated that the definition of this term in the IFR was unclear in part because it included many undefined terms. Commenters requested that the Department narrow the scope of the definition to exclude certain groups or industries, such as telecommunications carriers and transportation entities not engaged in the direct sale or purchase of ICTS.

The revised definition of ''party or parties to a transaction'' in this final rule is intended to clarify the types of activities in which a person would engage to be considered a party to a transaction. Specifically, this final rule amends the definition to provide that a party to a transaction is ''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.'' The new definition retains the existing exclusion for common carriers who operate without knowledge that they are providing transportation services of ICTS in connection with an ICTS Transaction that is prohibited or in violation of mitigation measures.

These changes are consistent with the reality that many of the risks related to ICTS Transactions result from the fact that the designer, developer, manufacturer, or supplier of the ICTS is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. This change also recognizes that, as described in the IFR and E.O. 13873, regardless of who receives the ICTS, it is possible that a single ICTS provider or class of ICTS designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary poses an undue or unacceptable risk to the United States or to U.S. persons. The change to the definition of ''party or parties to a transaction,'' in combination with changes to §§ 791.105 and 791.109 described below, is intended to better describe the parties the Department expects to identify in, and provide specific notice of, Initial and Final Determinations. These are the parties that have the greatest ability to control or address the risks identified in an Initial Determination, and therefore are the most appropriate parties for the Department's focus.

Nevertheless, the Department is not precluded from notifying the public at large or a targeted group of consumers of an Initial Determination, though it expects to do so only when an ICTS Transaction or party or parties providing ICTS present a national security risk that the Department believes must be addressed immediately. Notably, these changes preserve parties' ability to provide information to the Department about ICTS Transactions in which they engage.

(6) Definition of ''Person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary.''

The Department is making clarifying edits to the definition of ''person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary.'' Many commenters requested that the Department revise or clarify the definition, or the terms within the definition, of ''person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary,'' noting the potential breadth of entities covered by the definition.

Commenters specifically requested that the Department remove from the definition the language, ''any corporation, partnership, association, or other organization organized under the laws of a nation-state controlled by a foreign adversary'' because it could be construed to include U.S. companies' non-U.S. subsidiaries or operations located in foreign adversary countries. Commenters believed such a reading could cover intra-company transactions, and they did not view such subsidiaries and operations as posing any risk to U.S. national security or to the safety and security of U.S. persons.

This final rule retains the concept that an entity organized under the laws of a country controlled by a foreign adversary may be a person who is ''owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary.'' The Department understands commenters' concerns that U.S. companies' subsidiaries or operations located in foreign adversary countries may be considered subject to the jurisdiction or direction of a foreign adversary merely because of their location. However, the Department notes that the location of a U.S. entity's foreign subsidiary in the jurisdiction of a foreign adversary could pose a risk in some circumstances because the subsidiary might be required to comply with the rules, laws, or other requirements of that foreign adversary.

The Department believes that these commenters' concerns are addressed by the Department's procedures that require that the Secretary assess whether an ICTS Transaction falls within the scope of § 791.3(a) and § 791.103 before issuing an Initial Determination in connection with a transaction review. If the requirements of § 791.3(a) are met, the Secretary then assesses whether the 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
- Poses an undue or unacceptable risk under § 791.103.

The Department emphasizes that a foreign subsidiary's ICTS Transactions with its U.S. parent would be subject to further review only if those transactions present undue or unacceptable risks as identified in E.O. 13873 and under the criteria of § 791.103(c).

Other commenters expressed concern about the difficulty associated with determining whether a person is ''directly or indirectly supervised, directed, controlled, financed, or subsidized in whole or in majority part by a foreign adversary.'' Some questioned, for example, whether an ICTS Transaction by a U.S. citizen who resides in a foreign adversary country could be subject to review, or whether employing individual nationals of a foreign adversary country might make a U.S. company or its foreign subsidiaries ''subject to the jurisdiction or direction of a foreign adversary.'' These factors, commenters argued, could significantly impact the business models and outcomes for U.S. entities that conduct business in foreign adversary countries.

The Department is revising the definition to clarify that a U.S. citizen or permanent resident would not be considered a ''person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary'' merely due to dual citizenship, or residency in a country controlled by a foreign adversary. Moreover, the Department will carefully review particular ICTS Transactions connected to ''persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary'' that may pose an undue or unacceptable risk as identified in E.O. 13873 to account for the unique operations and risks specific to foreign adversary activities. The Department notes that if the Secretary finds as part of the initial review of a potential ICTS Transaction that it does not involve ''ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign

adversary,'' the transaction would no longer be under review. Therefore, absent other factors, mere participation in an ICTS Transaction by a U.S. person located in a foreign adversary or country controlled by a foreign adversary or by any individual national of a foreign adversary or country controlled by a foreign adversary would not be sufficient for the Secretary to continue a review because an ICTS Transaction must also pose an undue or unacceptable risk. For example, if a U.S. person uses a software application in a foreign adversary country, the ICTS Transaction would not necessarily be subject to review under the regulation if the software application was designed, developed, manufactured or supplied by a company that is not owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. Additionally, even if the software application were developed by a company that is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, the Department would not continue its review of an ICTS Transaction if it determined that the transaction does not pose an undue or unacceptable risk to the United States or U.S. persons as described in E.O. 13873. However, if a U.S. person designed, developed, manufactured, or supplied a software application in collaboration with a foreign adversary-controlled entity and the Department found that the acquisition, importation, transfer, installation, dealing in, or use of the software application may pose an undue or unacceptable risk, ICTS Transactions involving that software application would be subject to review under these regulations.

Regarding commenters' concern that a U.S. entity or foreign subsidiary of a U.S. entity might be considered ''owned by, controlled by, or subject to the jurisdiction or direction of'' a foreign adversary because it employs nationals of a foreign adversary country, the Department notes that, absent other indicia of ownership, control, or influence by a foreign adversary, solely employing nationals of a foreign adversary country would not independently trigger an ICTS Transaction review.

Several commenters noted that the IFR's definition of ''person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary'' was overbroad and did not meaningfully clarify which ICTS Transactions might be subject to review. Based on this feedback, the Department has revised the definition of ''person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary'' in this final rule to align with its original intent for the term's meaning. Specifically, the Department makes three clarifying edits to the definition. First, as noted above, the definition now makes clear that an individual would not be considered controlled by or subject to the jurisdiction of a foreign adversary solely due to their status as a citizen or resident of a foreign adversary or a country controlled by a foreign adversary, if that individual is also a U.S. citizen or permanent resident. Second, the Department clarifies that an entity may be subject to the jurisdiction of a foreign adversary if it has a principal place of business in, is headquartered in, is incorporated in, or is otherwise organized under the laws of a foreign adversary or a country controlled by a foreign adversary. Third, the definition now specifies that a person may be owned or controlled by a foreign adversary if another person that is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary possesses the direct or indirect power, 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. This change more directly reflects the Department's intent that, for example, foreign subsidiaries of U.S. companies or U.S. subsidiaries of foreign companies may in some cases be considered owned or controlled by a foreign adversary.

These edits address public comments expressing that the IFR's definition was confusing and unclear regarding the individuals or entities that might be ''owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary.'' The revisions also better align the definition with the type of persons that the Department would consider to be ''owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary,'' though the Department notes that a determination of the persons who meet this definition will be fact specific and made on a case-by-case basis.

(7) Definition of ''Appropriate agency heads.''

The Department received no comments on the definition of ''appropriate agency heads'' in the interim final rule but is revising the term in this final rule to make it clear that ''appropriate agency heads'' may refer to the designees of the agency heads listed in E.O. 13873. This addition is meant to clarify which officials may participate in the interagency notification and consultation processes described in §§ 791.104 and 791.108. This revision does not imply that agency heads must delegate any authority under E.O. 13873, but reflects current practice and will have no practical effect on the public or parties to an ICTS Transaction under review.

(8) Definition of ''Covered ICTS Transaction.''

This final rule adds a definition for the new term ''Covered ICTS Transaction,'' which was not defined in the IFR. This rule employs this new term to distinguish between transactions involving ICTS generally and ICTS Transactions that meet the criteria set forth in § 791.3. The new term ''Covered ICTS Transaction'' does not implement any substantive changes from the interim final rule, but is intended to clarify when the regulatory text refers to an ICTS Transaction, generally, and an ICTS Transaction that meets the criteria described in § 791.3 of the rule. For additional discussion of comments about defining terms used in § 791.3, see the preamble section below related to *Section 791.3 Scope of Covered ICTS Transactions.*

(9) Definition of ''Secretary.''

The Department is revising the definition of ''Secretary'' to identify the Under Secretary of Commerce for Industry and Security and the Executive Director of the Office of Information and Communications Technology and Services (OICTS) as designees to whom the Secretary may delegate authority under this final rule. Section 2(c) of E.O. 13873 permits the Secretary to redelegate within the Department the authority conferred on the Secretary pursuant to the E.O. Similar to the Department's revision of the term ''appropriate agency heads,'' this change reflects current practice and is meant to clarify which officials within the Department might be designated by the Secretary to take actions described in the regulation. This revision also addresses a question from commenters about which office within the Department will be primarily responsible for carrying out activities outlined in this final rule.

(10) Definition of ''United States person.''

This final rule adds ''any person in the United States'' to the definition of ''United States person'' to correct an inadvertent omission in the IFR. E.O. 13873 specifically defines the term

''United States person'' to mean ''any United States citizen, permanent resident alien, entity organized under the laws of the United States or any other jurisdiction within the United States (including foreign branches), or any person in the United States.'' This addition does not change the Department's practice, but it is intended to completely align the regulatory definition with the definition in E.O. 13873. Adding ''or any person in the United States'' ensures that persons who are not citizens or permanent resident aliens, but who are physically located in the United States, are considered ''United States persons'' as intended by E.O. 13873.

Section 791.3—Scope of Covered ICTS Transactions

The Department received many comments relating to the scope of the transactions covered by the interim final rule. Most of these commenters argued that the scope was too broad or not clearly defined, and commenters suggested that the rule could create burdens affecting technologies and ICTS Transactions that benefit the United States and chill routine and beneficial economic activity. Commenters also requested that the Department limit the scope of transactions covered by the rule to exclude activities already under review pursuant to existing regulations, and that the rule expand the existing exception for transactions reviewed by the Committee on Foreign Investment in the United States (CFIUS) to also include any ICTS Transaction by an individual or entity subject to a CFIUS mitigation agreement. Other commenters asked the Department to adopt a specific methodology for risk and threat analyses, and to review only those transactions with a ''strong nexus'' to the United States and that have the potential to have ''significant'' impacts on U.S. networks and infrastructure.

In this final rule, the Department declines to narrow the scope of transactions covered by the rule because it believes that the existing scope is appropriate and necessary to address undue or unacceptable risks as identified in E.O. 13873. E.O. 13873 describes the risk that certain ICTS Transactions could be used by malicious foreign actors to commit industrial or economic espionage, or that the unrestricted acquisition or use in the United States of ICTS with a foreign adversary nexus could be leveraged by foreign adversaries to find, create, and exploit vulnerabilities and undermine the resiliency of U.S. critical infrastructure or the safety and security of U.S. persons.

To protect U.S. ICTS supply chains from risks posed by malicious foreign actors' ICTS, it is necessary that the scope of transactions covered by this final rule encompass critical and emerging technologies and industries throughout the ICTS supply chain. The risks posed by ICTS Transactions are not always correlated with the transaction's scale and exist regardless of where or when the ICTS enters into the ICTS supply chain. The list of technologies in § 791.3 allows the Department to effectively address these risks by targeting different points of entry into the ICTS supply chain. The broad scope of § 791.3 gives the Department discretion to properly pinpoint and mitigate risks wherever they appear in the supply chain. The ICTS Transaction review process outlined in this final rule is consistent with the goals of E.O. 13873, while prioritizing the ICTS Transactions that pose the highest degree of undue or unacceptable risk, as identified in E.O. 13873, and minimizing the impact to digital and physical trade and commerce.

The Department notes that its reviews of transactions under the IFR have thus far been limited to the review of transactions involving all ICTS produced or provided by a single entity, rather than individual transactions between the entity and other parties, because the provision of ICTS by that entity was the basis of the undue or unacceptable risks. Therefore, the broad scope of the rule does not create undue burden but allows the Department to review ICTS Transactions to determine if an ICTS Transaction is in scope, pinpoint the source of the undue or unacceptable risk, and take action in the most efficient way to avoid tangential or unintended impacts on the U.S. economy or the ICTS supply chain.

In response to comments related to the CFIUS review exception, this final rule simplifies the language in § 791.3(b)(2) and consolidates the previous exception in § 791.3(b) and (c) of the IFR for CFIUS reviews, while preserving the safe harbor granted by CFIUS pursuant to its statute and regulations related to reviews of foreign investments into U.S. businesses and certain real estate transactions by foreign persons. ICTS Transaction reviews are limited to ICTS or classes of ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of one of the listed foreign adversaries, and the review of ICTS Transactions focuses on the undue or unacceptable risk posed by those ICTS Transactions. These reviews differ in scope from the focus on national security risk arising from certain transactions by foreign persons with or involving U.S. businesses or real estate under CFIUS. The revised provision in § 791.3(b)(2) clarifies that the Department will not review an ICTS Transaction that is also a covered transaction or covered real estate transaction under review, investigation, or assessment by CFIUS, or for which all action has concluded under section 721 of the Defense Production Act of 1950, as amended. This approach avoids duplicative reviews while eliminating potential gaps in mechanisms to review or address undue or unacceptable risks posed by transactions that are not or have not been in the CFIUS process. For the exception to apply, the ICTS Transaction must be the same transaction that CFIUS has determined is a covered transaction or covered real estate transaction under its authorities; a separate transaction, even if involving the same transaction parties subject to a CFIUS mitigation agreement, would not be subject to this exception. The mere fact that an individual or entity has participated in a CFIUS filing or is a party to a CFIUS mitigation agreement would not restrict the Secretary in reviewing *any* ICTS Transaction to which the individual or entity is party if the ICTS Transaction is distinct from the CFIUS transaction giving rise to a mitigation agreement. Otherwise, a foreign person that has obtained safe harbor for its investment into a U.S. company could then use that company to conduct or engage in malicious activities using ICTS Transactions that were not reviewed by CFIUS. Where CFIUS does not provide safe harbor with regard to the specific ICTS Transaction, the Department may review that ICTS Transaction for potential risks.

Several commenters requested that the Department implement additional exemptions or exclusions so that specific industries or technologies would not be subject to review under the rule. One commenter requested that arrangements for interconnection and the exchange of communications traffic (such as through fiberoptic cables) be exempted from the rule, while another noted that the rule should not be limited to any particular segment of the optical fiber communications industry. Other commenters sought exclusions in the rule for transactions involving information in the public domain, data transmission by telecommunication carriers on behalf of the general public, or technical research or standards development efforts. Others suggested

express safe harbor provisions for transportation companies like common carriers that merely transport ICTS, or safe harbors to create incentives to achieve ICTS supply chain security. Finally, several commenters requested clarification of the statement in the preamble of the IFR that ICTS Transactions solely involving personal hardware devices would not warrant particular scrutiny.

This final rule does not adopt any further exceptions or exclusions to the ICTS Transactions that would fall under § 791.3 of the rule. The Department notes that § 791.3 now refines the ICTS Transactions subject to further review by listing broad technology categories to indicate that the Department is concerned about ICTS Transactions involving information and communications hardware and software; ICTS integral to data hosting, computing or storage that uses, processes or retains sensitive personal data; connected software applications; ICTS integral to critical infrastructure; and ICTS integral to critical and emerging technologies. Section 791.3 is tailored to ensure that the regulations address risks posed by transactions involving the most critical elements and functions of ICTS. Therefore, the rule does not categorically exclude technologies, such as software operating on personal devices listed in E.O. 14034. In addition, the Department believes that the broad technology categories now included in § 791.3 address risks involving ICTS Transactions in the fiber communications and other industries by not implying that technologies that are not specifically listed as part of a category are excluded from possible review. The Department remains open to considering exclusions if further experience with the rule demonstrates that certain types of ICTS Transactions do not pose an undue or unacceptable risk as described in E.O. 13873 to national security, critical infrastructure, or U.S. persons.

Although this final rule does not implement suggestions to revise § 791.3 to exclude additional ICTS Transactions from the scope of transactions subject to review for prohibition or mitigation determinations, the Department has, in response to comments, simplified the list of technologies in § 791.3. In addition to improving clarity about the types of ICTS Transactions the Department may review, this final rule revises the list to focus on ICTS Transactions most likely to pose undue or unacceptable risks due to their foreign adversary nexus. The Department describes below additional changes in § 791.3 affecting the scope of transactions subject to review for prohibition or mitigation, broken out to provide clarity on each change and its corresponding rationale.

(1) Removal of One Million Unit or Person Threshold

This final rule removes the qualification that ICTS Transactions that involve the use, processing, or retention of sensitive personal data must include the data of more than one million U.S. persons to be subject to review. Additionally, this final rule removes the one-million-unit sales minimum for internet-enabled sensors, webcams, or other end-point surveillance or monitoring devices; routers, modems, or any other home networking device; or drones or other unmanned aerial systems. This final rule also removes the qualification that software designed primarily for connecting with and communicating via the internet be in use by over one million people to be considered ICTS for the purposes of the rule. The Department did not receive many comments regarding these provisions, except to note that it is common for multinational companies to collect and retain data on more than one million individuals and to request an explanation of how the Department would calculate whether a transaction met the numeric threshold.

The Department is removing these thresholds in § 791.3 because the use of a threshold to review an ICTS Transaction is not necessary. The numerical threshold served as a proxy for ''undue or unacceptable risk'' under the rationale that only transactions involving a large number of sales or users would constitute a true national security risk. However, numerical thresholds do not necessarily correlate with the risks presented by ICTS Transactions involving sensitive personal data. It is possible, for example, that an ICTS Transaction that results in the storage, retention, or use of sensitive personal data of relatively few U.S. persons (such as persons with restricted access to sensitive governmental information) could result in significant risks to U.S. national security or to the safety and security of U.S. persons. Furthermore, as one commenter pointed out; there is nothing inherently riskier about collecting, storing, or retaining data on a specific number of people, or of a certain number of sales. Put another way, the risks presented by ICTS Transactions involving sensitive personal data relate to the type of data collected and the identity of persons from whom that data is collected, rather than the volume of transactions. Moreover, the Secretary, with other appropriate agency heads, is separately tasked with evaluating the national security risk. That evaluation may include, as one factor, the number of sales or users.

Limiting review of transactions to only those that involve a certain number of users, units, or sales, would be contrary to the objective articulated in E.O. 13873 to reduce, remove, or minimize the risks posed by certain ICTS Transactions, as it would fail to address significant risks posed by ICTS Transactions that fall below the existing thresholds, especially where those ICTS Transactions involve sensitive personal data. Furthermore, such thresholds could result in strategic circumventive behavior by malicious foreign actors who might attempt to limit ICTS Transactions involving sensitive personal data or otherwise posing risks under a particular threshold so as to evade review. For these reasons, the Department is eliminating the thresholds referencing one million persons, units, or sales.

(2) Connected Software Applications

In addition to the changes noted above, the Department is consolidating the examples of software applications from what was § 791.3(a)(4)(v)(A) through (D) into revised § 791.3(a)(4)(iii) to clarify that desktop, mobile, gaming, and web-based applications are all non-exclusive examples of connected software applications that are subject to this final rule, so as to not suggest that those applications are distinct from connected software applications. This revision is consistent with E.O. 14034 but is not a substantive change from the interim final rule.

(3) Definitions of Terms Related to Covered ICTS Transactions

Several commenters requested that the Department clarify the meaning of certain phrases used in § 791.3. First, some commenters proposed that the Department define the phrase ''any person subject to the jurisdiction of the United States'' in § 791.3(a)(1) to have the same meaning as ''United States person,'' which they argued would clarify the status of foreign subsidiaries of U.S. companies. Alternatively, commenters suggested the term be defined to include only transactions in which the ICTS enters the United States or is used in the United States.

This final rule uses the phrase ''person subject to the jurisdiction of the United States'' in § 791.3(a)(1) because that is the phrase used in E.O. 13873. Specifically, section 1 of the E.O. describes the scope of conduct subject

to prohibition as transactions ''by any person, or with respect to any property, subject to the jurisdiction of the United States.'' Therefore, this final rule does not change the phrase ''person subject to the jurisdiction of the United States'' in § 791.3(a)(1), which is meant to reflect the language and the requirements of E.O. 13873, to remain consistent with the Department's authorities under E.O. 13873.

Additionally, some commenters requested an explanation of the meaning of the term ''integral'' as it was used in § 791.3(a)(4)(ii), (iii), and (vi). However, like the IFR, this final rule uses ''integral'' in § 791.3 consistent with the word's common meaning as something that is important or necessary for the operation of ICTS. The Department believes it is not necessary to further define the term ''integral'' beyond its commonly understood meaning, because any such attempt might add to rather than reduce confusion and might widen or narrow the scope of the rule in ways detrimental to the Department's ability to identify and address risks.

Finally, a commenter asked the Department to define the term ''interest'' in § 791.3(a)(2). That provision states that the rule applies to ICTS Transactions that involve ''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).'' The commenter stated that, without a definition, the term ''interest'' could make ICTS Transactions in which a foreign person has only a tangential, non-controlling interest subject to Departmental review. However, unless an ICTS Transaction also involves ''ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary'' under § 791.103(b), a foreign person's tangential interest in property alone would not be sufficient to warrant review by the Secretary. The Department does not provide a general definition for the term ''interest.'' To explain the term as it is used in section 791.3, the Department is adding language in § 791.3(a)(2) to clarify that the Secretary may review any ICTS Transactions that involve any property in which a foreign national or foreign country has any direct or indirect interest of any nature whatsoever. In the context of § 791.3, the term ''interest'' includes any interest whatsoever, direct or indirect. This is similar to the term ''interest'' as defined by the Office of Foreign Assets Control, which also include any interest whatsoever, direct or indirect.

(4) Critical Infrastructure

One commenter requested that the Department provide guidance on the sectors that are included in the term ''critical infrastructure'' and suggested that the Department draw on definitions in CFIUS regulations for this definition. Like the IFR, this final rule continues to use an Executive Office of the President publication to identify critical infrastructure sectors. The IFR considered ''critical infrastructure'' sectors as those identified in Presidential Policy Directive 21—Critical Infrastructure Security and Resilience (PPD–21), and the final rule continues to identify the almost identical sectors that are listed in National Security Memorandum 22 on Critical Infrastructure Security and Resilience (NSM–22). However, whereas the IFR referred to the sectors designated as critical infrastructure by PPD–21, § 791.3 of this final rule specifically lists the individual critical infrastructure sectors identified in NSM–22 in § 791.3(a)(4)(iv) to provide additional clarity to the public. NSM–22 includes subsectors of the designated critical infrastructure sectors, and the Department may consider revising the list in § 791.3(a)(4)(iv) to conform to future changes related to critical infrastructure sectors identified in NSM–22. A further description of these sectors can be found here: *https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/*. Additional details on critical infrastructure sectors are also available at the U.S. Department of Homeland Security's Cybersecurity & Infrastructure Security Agency's website, *https://www.cisa.gov/*. NSM–22 uses a similar definition of ''critical infrastructure'' as CFIUS, though the Department is not adopting the commenter's suggestion to use the definition of the term ''critical infrastructure'' directly from CFIUS regulations. By listing the sixteen critical infrastructure sectors identified in NSM–22, the Department provides guidance to stakeholders about which sectors are of particular concern to the Department and represent the Department's highest priority.

(5) List of Critical and Emerging Technologies

Certain commenters expressed concern that specific critical and emerging technology categories in § 791.3 were too broad, and recommended that only facets of particular critical and emerging technologies should be specifically identified. In this final rule, the Department is not narrowing the scope of specific critical and emerging technologies but notes that the primary concern is with ICTS Transactions that pose undue or unacceptable risks related to critical and emerging technologies, as opposed to critical and emerging technology in general. The Department is amending the list of critical and emerging technologies in § 791.3(a)(4)(v) to indicate that the Department is not solely concerned about artificial intelligence and machine learning; quantum key distribution; quantum computing; drones; autonomous systems; or advanced robotics. Rather, the Department is concerned about potential situations where ICTS Transactions involving critical and emerging technologies with a foreign adversary nexus may pose undue or unacceptable risks to U.S. national and economic security. While quantum information and enabling technologies, artificial intelligence, autonomous systems, advanced robotics, and drones remain in scope, the critical and emerging technology list now includes eleven technology categories to reflect technological advancements and changes in the risk landscape since the Department issued the IFR. The list of eleven technologies is based on a comparison of common technologies between the 2023 United States Government National Standards Strategy for Critical and Emerging Technology and the White House's Office of Science and Technology Policy 2024 list of Critical and Emerging Technologies.

(6) Retroactivity of Rule's Applicability

Under § 791.3, the regulations apply to ICTS Transactions that were initiated, pending, or completed on or after January 19, 2021. Several commenters were concerned that an investigation could require parties to divest entities or ''unwind'' long closed transactions. These commenters asserted that review of closed transactions could increase uncertainty for industry, disrupt ongoing business relationships, and deter U.S. innovation and technology investment.

Some commenters raised concerns about the retroactive application of the regulations to services under contract prior to January 19, 2021. A common example cited by commenters was the potential investigation of a transaction involving services provided under a purchase order or statement of work pursuant to a master service agreement entered by the parties prior to January 19, 2021. Commenters were concerned that the Department's review could

disrupt the underlying service contract and requested that such arrangements be excluded from review.

The Department reiterates that this final rule does not apply retroactively to transactions that were completed prior to January 19, 2021. Nevertheless, under this final rule, the Department may review ICTS Transactions initiated, pending, or completed on or after January 19, 2021, even if they are related to a contractual or other agreement established prior to January 19, 2021. While the regulations could change expectations about how parties' multi-year arrangements would operate relative to before the rule took effect, the regulations nevertheless only apply to ICTS Transactions initiated, pending, or completed on or after January 19, 2021.

To clarify, using an example provided by commenters: ICTS obtained using a purchase order dated on or after January 19, 2021, may be subject to review by the Secretary, even if an agreement regarding the provision of such ICTS was established prior to the purchase order date. This is because the provision of ICTS after January 19, 2021, is considered a new ICTS Transaction that is distinct from the underlying contract. If reviews were limited to only transactions with no connection to business arrangements entered into prior to January 19, 2021 the Department would be prevented from examining and mitigating or prohibiting ongoing risks arising from the current provision of ICTS. Thus, like the IFR, this final rule provides that new activity—for example, provision of ICTS, service updates, or operations—under contracts that existed on or prior to January 19, 2021, constitute new ICTS Transactions that may be subject to review.

The Department's experience to date has involved reviews focused on systemic risks posed by classes of ICTS Transactions involving a particular ICTS provider, rather than risks posed by individual ICTS Transactions. The risks arising from such ICTS Transactions exist regardless of when a contract may have been entered into, and in fact the risks might persist because of such contracts. Therefore, under this final rule, the Department may review ICTS Transactions that occur after January 19, 2021, even if they occur pursuant to a contract or agreement entered into prior to that date.

Some commenters explained that—even for contracts initially entered after January 19, 2021—an investigation initiated by the Department several years after an arrangement's effective date could require the termination of long-settled business relationships. These commenters requested that the Department establish a statute of limitations of sorts, establishing a time limit beyond which the Department could not review an ICTS Transaction. However, the Department's reviews are focused on the timely elimination or mitigation of undue or unacceptable risks as identified in E.O. 13873, and changed circumstances over time may affect the risks posed by a closed transaction. Therefore, this final rule does not establish a limitations period separate from the statute of limitations for violations of IEEPA because the Department's experience with the procedures set out in the regulations has not suggested that implementing a fixed limitations period is necessary.

Section 791.4—Determination of Foreign Adversaries

Some commenters raised concerns about the process in § 791.4 by which the Secretary determines foreign adversaries. These commenters argued that the process is unclear and could potentially be overly broad. Some commentors requested that the Department provide additional information about the criteria used to determine foreign adversaries, publish unclassified information supporting the Secretary's determination of foreign adversaries, or provide prior notice before any revisions to the Secretary's determination of foreign adversaries under § 791.4 take effect. Others requested that the Secretary focus on specific entities or persons rather than foreign governments, and another commenter requested that the Department exclude governments with whom the United States has a defense treaty alliance from designation as a foreign adversary. The commenters stated that these suggested revisions would avoid disproportionate responses to potential risks and would allow stakeholders time to comply with new regulatory requirements.

This final rule does not revise or amend the provisions on determinations of foreign adversaries, nor is the Department proposing specific procedures for such determinations. Although the Department appreciates commenters' desire for clarity about the determination process, a requirement for the Secretary to follow specific procedures in making a determination could undermine the security and safety of the United States, as a foreign adversary determination indicates that those entities pose significant risks to U.S. national security. Nonetheless, any new foreign adversary determination would apply only to actions taken after such a determination.

Regarding commenters' request that certain governments be excluded from designation as foreign adversaries, such as those with whom the United States has a defensive treaty alliance, or that the Department not designate entire governments as foreign adversaries, the Department notes two points. First, that the definition of ''foreign adversary'' in E.O. 13873 includes foreign governments and foreign non-government persons and is not subject to revision by this final rule. Second, E.O. 13873 grants the Secretary discretion to consider all aspects of entities before determining whether they are a ''foreign adversary'' that should be listed in the regulation. The Department declines to categorically exclude certain types of entities from possible foreign adversary determinations because doing so could limit the Department's ability to address future risks facing the ICTS supply chain.

Although this final rule does not exclude any foreign governments or foreign non-government persons from § 791.4 in response to comments, it does correct the definition to include the ''Macau Special Administrative Region'' in § 791.4(a)(1) within the People's Republic of China in the list of foreign adversaries. Section 791.4(a)(1) is updated to read ''The People's Republic of China, including the Hong Kong Special Administrative Region and the Macau Special Administrative Region (China).'' Macau is a part of the People's Republic of China, just as is Hong Kong, and should be included in the definition to remove any uncertainty as to the geographic scope of the term.

Section 791.100—Information Available to the Secretary

Several commenters expressed concerns that the Department may initiate an ICTS Transaction review solely on the basis of a referral of information from industry, and that accepting such referrals may encourage anti-competitive behavior. In response, the Department has updated § 791.100(a)(8) and (9) in this final rule to distinguish between a referral from another U.S. Government agency and information from private industry provided voluntarily. This final rule uses the term ''referral'' to mean information from or a recommendation made by other U.S. Government agencies to the Department. In some cases, information provided by an industry entity may assist the Department in assessing an ICTS Transaction and the potential risks such transactions may pose to U.S. national security or U.S. persons, and the

Department would not reject that information. Even so, the Department emphasizes it does not encourage abuse of its processes for anti-competitive purposes. As with all information received by the Department, the Department will carefully vet information provided voluntarily by private industry pursuant to § 791.100(a)(9). This information will be treated holistically and will be used in the same ways as other information that is generally available to the U.S. Government.

Additionally, some commenters requested further explanation of how the Secretary will assess 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 under § 791.100(c). Specifically, commenters requested that the Department define ''ties between the person—including its officers, directors or similar officials, employees, consultants, or contractors—and a foreign adversary,'' in § 791.100(c)(2). Some suggested that ''ties'' be defined to mean that a person is a business partner, close associate, or family member of a foreign adversary. The Department believes that § 791.100(c) currently captures the relationships that the Secretary may consider when assessing whether a 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 that limiting the Secretary's consideration as suggested by commenters could hinder the Secretary's ability to appropriately respond to risks in a given case.

Section 791.101—Information to be Furnished Upon Demand

The IFR specified that ''persons involved in an ICTS Transaction'' may be required to furnish information under oath. In this final rule, the Department updates § 791.101 to note that, pursuant to the authority granted to the Department by E.O. 13873 and IEEPA, the Department may require any person to furnish, under oath, complete information relative to a transaction involving ICTS. This revision is made to better reflect the authorities granted to the Department under IEEPA and E.O. 13873.

Section 791.102—Confidentiality of Information

While generally supportive of the interim final rule's confidentiality provisions, a few commenters stressed that confidential information provided to the Department should not be disclosed publicly. Other commenters requested that the rule clearly establish the obligations of any third-party contractors to protect confidential information.

The Department appreciates these comments and the need to protect business confidential information or other sensitive information from disclosure, particularly as such information may be necessary for the Department to assess potential or actual risks related to ICTS Transactions or classes of ICTS Transactions. The Department believes that these confidentiality concerns are addressed by the protections for such information already afforded in § 791.102, along with the applicable disclosure exemptions under the Freedom of Information Act and criminal penalties for Federal employees who disclose business confidential information (18 U.S.C. 1905).

This final rule implements a few changes to § 791.102. First, it removes duplication within § 791.102(b) to make clear that all potential disclosures pursuant to the regulations of information or documentary materials that are not otherwise publicly or commercially available would be ''subject to appropriate confidentiality and classification requirements.'' It also revises § 791.102(b)(4), correcting an inadvertent typographical error in the IFR to permit the Secretary to disclose confidential information in response to ''a request by'' a governmental entity or a foreign government entity of a U.S. ally or partner, but only to the extent such disclosure is necessary for national security purposes.

Second, this final rule amends § 791.102(b)(6) to provide that, when otherwise permitted by law, the Secretary may disclose information or documentary materials that are not otherwise publicly or commercially available if necessary to prevent imminent harm to U.S. national security or the security and safety of U.S. persons. The Department anticipates that disclosure of information under this paragraph would only occur in the exceptional case where public or commercially available information would not suffice to prevent an imminent and specifically identified harm.

Section 791.103—Review of ICTS Transactions

The Department received several comments about the Secretary's review of ICTS Transactions under § 791.103. Commenters generally raised concerns about the breadth of these provisions and sought greater clarity in the procedures the Secretary will follow when determining whether to initiate review of an ICTS Transaction. One commenter suggested that the initial review of the risks posed by an ICTS Transaction should include an analysis of the potential costs that would be required to remediate any identified risks. Several commenters questioned the circumstances under which the Secretary should be able to consider referrals for review of ICTS Transactions or classes of ICTS Transactions based on information received from private parties due to the potential for anti-competitive behavior. Those commenters provided multiple suggestions, including to eliminate the option for the Secretary to consider a transaction based on information submitted by private parties, implementation of a process for entities to review and respond to information from private parties that prompts review of a transaction, or a requirement that any private party submitting information that prompts a review also provide a sworn affirmation that the information supplied is true and correct.

As noted above in the discussion of *Section 791.100 ''Information Available to the Secretary,''* the Department will consider all available information when reviewing an ICTS Transaction, including information received from private industry. The Secretary critically assesses all information received during a transaction review. Specifically, as outlined in § 791.103, the Secretary will assess whether an ICTS Transaction falls within the scope described in § 791.3, 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 poses an undue or unacceptable risk as described in §§ 791.100(d) and 791.103(c).

In response to commenters' concerns about anti-competitive conduct in connection with ICTS Transaction reviews initiated following the receipt of information from industry, as discussed further below, this final rule amends § 791.105 to clarify that the Secretary will provide a party or parties to a transaction with information regarding the factual basis supporting the Secretary's Initial Determination. Section 791.107 affords parties an opportunity to respond to the Initial Determination and identify potential errors in that document or argue that the circumstances leading to the Initial Determination no longer apply, prior to the Secretary taking any final action.

Accordingly, pursuant to § 791.107, if the parties believe that information used for the Initial Determination is incorrect, the parties can correct that information during the response period. Consistent with the approach outlined above to address commenters' concerns about anti-competitive acts by parties, the Department expects that § 791.200, which authorizes penalties for, among other acts, submitting false or fraudulent statements to the Department, will deter submissions of false information for anti-competitive purposes.

This final rule also includes several procedural changes to § 791.103. First, this final rule revises § 791.103(a) to clarify that the Secretary has the discretion to initiate review of an ICTS Transaction after considering any of the information described in § 791.100(a), including referrals from other U.S. Government agencies. Section 791.103(b) specifies that the Secretary will make determinations during this review about whether a transaction is a Covered ICTS Transaction as described in § 791.3, involves ICTS that is 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 poses an undue or unacceptable risk as identified in E.O. 13873 and described in §§ 791.100(d) and 791.103(c). In assessing whether an ICTS Transaction poses an undue or unacceptable risk, the Secretary may evaluate the criteria listed in § 791.103(c) and the materials described in § 791.100(d). These revisions to § 791.103(a) and (b) in this final rule do not reflect substantive changes from the IFR, but the revisions clarify that, consistent with E.O. 13873, the Secretary may commence a review on the Secretary's own initiative or following a referral from another U.S. Government agency.

In addition, this final rule revises § 791.103(c) regarding the criteria the Secretary may consider when evaluating whether a Covered ICTS Transaction poses an undue or unacceptable risk. To provide more detail and to acknowledge the potential economic impacts of actions under this rule, this final rule amends § 791.103(c)(7), which previously specified that the Secretary would consider the ''nature of the vulnerability implicated by the ICTS Transaction,'' to state that the Secretary will consider the ''nature and characteristics of the customer base, business relationships, and operating locations of the parties to the Covered ICTS Transaction.'' Additionally, to streamline criteria that the Secretary will use to assess undue or unacceptable risks posed by covered ICTS Transactions, § 791.103(c) now combines certain aspects of the criteria for evaluating connected software applications listed in E.O. 14034 with the criteria for all other types of ICTS Transactions, when applicable. Under this final rule, the criteria previously listed in the IFR's § 791.103(d)(1), (3), and (4) related to connected software applications are now included in § 791.103(c)(2), streamlining the regulatory text and eliminating redundancies. Specifically, for all ICTS Transactions the Secretary may evaluate the ownership, control, or management by persons subject to the jurisdiction or direction of a foreign adversary, including connections to foreign adversary military and connections to persons involved in malicious cyber activities.

The criteria that specifically apply to connected software applications are now listed under § 791.103(c)(11), and the list consists of:

- The number and sensitivity of users;
- The scope and sensitivity of data that the application collects;
- Use of the connected software application to conduct surveillance that enables espionage;
- Regular, reliable third-party auditing of the application; and
- The extent to which identified risks can be mitigated and verified.

This reorganization clarifies the factors that the Secretary may evaluate when determining whether ICTS Transactions involving connected software applications pose undue or unacceptable risks pursuant to the authority granted by E.O. 14034, and it better integrates the criteria that may be relevant to reviews of ICTS Transactions involving connected software applications as well as to reviews of other ICTS Transactions.

Section 791.104—Interagency Notification

Several commenters expressed uncertainty about the interagency consultation requirements in the IFR. Some suggested that the Department should further explain the meaning of ''interagency consultation'' mentioned in §§ 791.104 and 791.108, noting that the IFR did not establish a formal consultative process. Other commenters recommended that the rule specifically reference other agency or executive department heads for inclusion in the consultation process to avoid duplicative reviews of ICTS Transactions, particularly in the context of government procurement. Commenters also requested a definition of the term ''consultation'' to ensure it is more than a ''mere notification'' to other agencies, and that it require an interagency vote and interagency consensus on whether an ICTS Transaction is subject to the rule prior to elevating any disagreement to the President. Commenters argued that consensus-seeking would ensure a ''whole of government'' approach to addressing ICTS Transactions and avoid duplicate or conflicting actions taken by the agencies tasked with securing ICTS. In response, this final rule makes several changes to clarify the nature of the consultations with other agencies required prior to Initial Determinations and Final Determinations.

Consultations between agencies can take many forms and may have different meanings or requirements in specific contexts. Consultation may be ''formal,'' or ''informal,'' and result in a memorandum of agreement between agencies, written decisions, or more informal understandings or discussions between agencies. The IFR required consultation in certain circumstances but did not describe what such consultation would entail. In this final rule, the Department amends the consultation provisions to better describe the types of interagency consultation required prior to the production of the Initial Determination and the issuance of the Final Determination.

This final rule amends § 791.104 (Initial Determination) and § 791.108 (Final Determination) to clarify what is required of the Department and the appropriate agency heads during the processes prior to issuing Initial or Final Determinations. These changes are procedural in nature and will have a limited impact on the public or the parties to a transaction under review. The changes do not expand the list of agency heads included in the definition of ''appropriate agency heads,'' because the list consists of agencies specifically identified in E.O. 13873. Both the E.O. and this final rule provide that, where the Secretary determines it to be appropriate, other agency heads may be consulted, which allows for sufficient latitude to avoid redundant regulatory efforts.

This final rule amends § 791.104 to describe the Secretary's process of notifying and receiving comments from appropriate agency heads if the Secretary assesses that an ICTS Transaction meets the criteria in § 791.103. If the Secretary assesses that an ICTS Transaction meets the criteria described in § 791.103(b), as part of the consultation process the Secretary will

notify the appropriate agency heads of such and provide each agency head the opportunity to submit to the Department, within 21 days, any comments in writing regarding the assessment. If an agency head does not provide written comments within that time, the Secretary may presume that the agency has no comments. Under this final rule, as under the IFR, if an agency head provides comments, the Secretary may use those comments to inform further assessment of whether the ICTS Transaction meets the criteria in § 791.103 and to inform the development of the Initial Determination issued under § 791.105. In such circumstances, if an agency head disagrees with the Secretary's assessment, the Secretary will carefully consider the agency head's position in determining how to proceed. The Department will notify appropriate agency heads of an Initial Determination at least twenty-one (21) calendar days prior to issuing and notifying a party or the parties to the Covered ICTS Transaction of the Initial Determination under § 791.105(b)(3).

E.O. 13873 does not require the Secretary to seek consensus from the appropriate agency heads prior to issuing an Initial Determination and this final rule does not add a consensus requirement to § 791.104. However, in all cases, the Secretary will carefully weigh the comments received from appropriate agency heads and will consult with the appropriate agency heads to avoid redundant regulatory efforts.

The amendments to § 791.108 in this final rule, covering the interagency consultation regarding the Final Determination, are discussed in more detail below in the discussion of *Section 791.108* ''*Interagency Consultation on the Final Determination.*''

Section 791.105—Initial Determination

The interim final rule established a process for the Secretary to issue an Initial Determination in § 7.105. The Department received relatively few comments addressing this section of the rule, but some commenters requested that the Department amend §§ 791.105 and 791.109(f) to strike provisions authorizing publication of the Initial Determination or Final Determination in the **Federal Register**, to require the Department to omit from public notices information that would reveal the identities of the parties to an ICTS Transaction, or to require party consent before publication in the **Federal Register**. Commenters acknowledged that the rule does not generally permit public disclosure of confidential information, but some argued that the Initial Determination and Final Determination should themselves be treated as confidential and noted that publication of the Secretary's determinations could lead to financial or reputational harm.

In consideration of the comments about publication of Initial Determinations, the Department is revising § 791.105(d) to note that the Secretary retains discretion to publish a notice of an Initial Determination—rather than the full text of an Initial Determination—in the **Federal Register**. The Department is committed to appropriately safeguarding confidential information in its possession and, when possible, mitigating unnecessary economic impact to parties to an ICTS Transaction. While some commenters asserted that, in all situations, Initial Determinations and Final Determinations should not be made public, the Department maintains its discretion to publish notices of Initial Determinations in the **Federal Register** when warranted; for example, to mitigate undue or unacceptable risks, or when an ICTS Transaction significantly impacts members of the public.

The Department disagrees with commenters who maintain that, if the Department publishes a notice of an Initial Determination in the **Federal Register**, the names of parties should be omitted from the notice. Because Initial Determinations do not represent final decisions, and because the Department recognizes that there may be an economic impact on parties named in those publications, the Department may choose not to publish notices of Initial Determinations in the **Federal Register**. However, the Department may choose to do so in certain situations, particularly when non-parties or parties that cannot be individually identified will be affected by a determination, such as when classes of ICTS Transactions are involved. The discretion to publish Initial Determinations, including the names of parties, allows the Department to address situations in which national security risks are significant or imminent and publication will assist the public, including U.S. businesses, in avoiding those risks.

In such cases, publishing a notice of an Initial Determination in the **Federal Register** allows for such persons to receive notice of a decision. In the circumstance in which the Department decides to publish a notice of an Initial Determination, the Department would also publish a notice of a Final Determination to inform the public of the final outcome of its review.

This final rule amends § 791.105(a) and (b) to reflect the new interagency notification procedures in § 791.104. These revisions explain that the Secretary will consider comments received from appropriate agency heads regarding the Secretary's assessment of whether an ICTS Transaction meets the criteria under § 791.103(b). However, the Secretary retains discretion to determine whether the transaction poses an undue or unacceptable risk and, therefore, the discretion to end review of an ICTS Transaction, amend the assessment, or proceed to making an Initial Determination.

This final rule also amends § 791.105(b)(1) to note that the Initial Determination will provide parties with information regarding the factual basis supporting the Secretary's decision to either prohibit an ICTS Transaction or permit the ICTS Transaction with mitigation measures. This clarification will ensure that parties receive notice of the material facts underlying the Secretary's Initial Determination and will help parties provide more specific and complete responses to the Secretary's Initial Determination under § 791.107. As discussed previously, this revision also responds to comments requesting that the rule provide parties an opportunity to respond to information that private parties submit to the Department. These changes allow for parties to review and respond to facts submitted by private parties when such information is part of the factual basis supporting an Initial Determination.

In addition, this final rule modifies § 791.105(b)(3) to clarify how the Department identifies parties to an ICTS Transaction that must be served with an Initial Determination. New § 791.105(b)(3)(i) addresses the situation in which the Department identifies a limited number of parties to a single or set of ICTS Transactions who would be served the Initial Determination. New § 791.105(b)(3)(ii) addresses situations, which the Department expects will be common, in which the Department reviews a class of ICTS Transactions involving a single person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as well as unidentified U.S. persons or U.S. persons whom it is not practical to identify. These situations may involve a large number of U.S. consumers, many of whom cannot be individually identified or whom it would be impractical to individually identify. In such case, individual service of the Initial Determination on every party may not be feasible or may be unnecessary or inappropriate. The

unknown or unidentifiable U.S. parties in many cases will not have unique information that would affect the Final Determination or, for example, enable the Department to negotiate effective mitigation measures. New § 791.105(b)(3)(ii) therefore recognizes that seeking to notify all potential parties who have purchased or accessed ICTS that the Department deems to entail undue or unacceptable risk may not be possible or practical, nor would it help the Department to mitigate or eliminate risks associated with the ICTS.

The Department may still publish a notice of an Initial Determination in the **Federal Register**, pursuant to § 791.105(d), where, for example, notice would be beneficial to warn the public about an identified risk. These changes to § 791.105(b)(3) and (d) are procedural in nature. The Department will employ the method of service that is best suited to notifying the affected parties to an ICTS Transaction and provide them with an opportunity to respond to an Initial Determination.

Section 791.106—Recordkeeping Requirement

The Department received no comments about the recordkeeping requirements in § 791.106. This final rule revises § 791.106, based on the Department's experience, to provide examples of the types of notification that require notified individuals or entities to retain records related to an ICTS Transaction, and to implement a time limit for record retention. In addition to directly notifying a person that an ICTS Transaction is under review, the Department may notify a person through other means, such as a demand for information or documents under § 791.101. Under revised § 791.106, upon receipt of this notification, a person must promptly take steps to retain records related to the identified ICTS Transaction. Revised § 791.106 also clarifies that any records that a notified person must retain in connection with an ICTS Transaction must be retained for ten years following issuance of a Final Determination unless the Final Determination specifies otherwise. Instead of retaining the interim final rule's indefinite record retention requirement, the Department intends for the ten-year time limit to reduce any costs associated with record retention pursuant to the rule. If the Department does not issue an Initial Determination to a person within ten years of providing notice that an ICTS Transaction is under review, that person can assume their recordkeeping obligation has been satisfied unless otherwise informed by the Department.

Section 791.107—Procedures Governing Response and Mitigation

The interim final rule provided that, after being notified of an Initial Determination, parties to an ICTS Transaction would have 30 days to respond to the Initial Determination or to assert that the circumstances resulting in the Initial Determination no longer apply. Several commenters expressed concern that the time provided in § 791.107 for a party's response to the Secretary's Initial Determination was not long enough. Commenters explained that it may take a party to an ICTS Transaction longer than 30 days to respond or propose mitigation measures if the issues or business relationships identified in an Initial Determination are particularly complex. Some commenters also requested a maximum timespan for imposed mitigations, or a periodic review of the mitigation measures to determine whether they should remain in effect.

This final rule does not establish a maximum timespan for imposed mitigations because the Department continues to believe that such an across-the-board maximum would hinder the Department in fully evaluating any implemented mitigations, resulting in national security vulnerabilities. Risks will be specific to each case, and because the rule provides that the Department may negotiate mitigation measures with the parties to an ICTS Transaction, the mitigation measures (when applicable) will also be specific to each case and tailored to address the identified risks. In some cases, a mitigation measure might be appropriate for a limited time; in other cases, a limited time frame might merely delay the realization of the identified risks or even increase them. Furthermore, under § 791.6, which states that ''any determinations, prohibitions, or decisions issued under this part may be amended, modified, or revoked, in whole or in part, at any time,'' the Secretary is already permitted to modify mitigation measures when necessary or appropriate. Therefore, the Department believes that amending the rule as suggested by these comments is unnecessary.

However, this final rule does make several changes to the procedures governing response and mitigation in § 791.107, including some minor stylistic edits. Because 30 days may not always be sufficient time for a party to prepare a response to the Initial Determination or propose remedial steps, this final rule amends § 791.107, in response to comments, to allow an initial 30 days to respond to an Initial Determination. Additionally, § 791.107 allows parties to seek, and the Secretary to allow for good cause shown, an extension of another 30 days. In total, parties may receive up to 60 days to respond to an Initial Determination (30 days initially with a potential 30-day extension). The Secretary retains discretion to grant an extension and may consider factors such as the complexity of the ICTS Transaction under review, the severity of the risks identified in the Initial Determination, and the impact that granting an extension might have on the overall timeframe for review.

Additionally, this final rule amends § 791.107(c) to clarify that all written submissions from a party in response to an Initial Determination may not exceed 50 pages unless a party obtains prior approval from the Secretary. The Department believes that a page limit will facilitate more efficient communications between the Department and the party or parties to an ICTS Transaction. The Department also clarifies in new § 791.107(c)(3) that parties may include business confidential information in written submissions to the Department, but that any business confidential information included in a submission must be clearly and specifically identified. The clear demarcation of business confidential information in parties' submissions will help the Department be responsive to concerns raised by commenters about protecting this type of information.

Section 791.108—Interagency Consultation on the Final Determination

In response to comments expressing uncertainty about the process the Secretary will use to consult with appropriate agency heads regarding a proposed Final Determination, this final rule amends § 791.108 to provide the public with more clarity about the procedures governing the interagency consultation on the Final Determination.

E.O. 13873 requires the Secretary to consult with appropriate agency heads when 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, whether the ICTS Transaction poses an undue or unacceptable risk, and when designing or negotiating measures to mitigate the risks posed by an ICTS Transaction that would otherwise be prohibited. The IFR

implemented the directive in E.O. 13873 for the Secretary to make certain determinations ''in consultation'' with heads of agencies by specifying in § 791.108 that the Secretary would ''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.'' However, as commenters noted, the IFR did not clearly explain that consensus requirement.

This final rule clarifies the requirement for the Secretary to seek the concurrence of all appropriate agency heads before issuing a Final Determination. With this final rule, the Secretary may presume concurrence if no response is received within fourteen days from one of the appropriate agency heads or the designee of appropriate agency heads. This final rule also clarifies that if an agency objects to the Final Determination, the objection must be received by the Secretary within the 14 days, and the objection must come from the agency's Deputy Secretary or equivalent level.

Under the final rule, the Secretary will consult with and seek concurrence of appropriate agency heads and will carefully consider views from the appropriate agency heads to inform a Final Determination. The Department has established procedures to ensure robust interagency participation in the process. Consultation will allow the Secretary to update Final Determinations based on interagency input.

Section—791.109 Final Determination

Section 791.109 sets forth the process the Secretary will follow when issuing a Final Determination and the information that must be included in the Final Determination. Section 791.109(b) of the interim final rule required the Secretary, absent a finding that additional time is necessary, to issue a Final Determination within 180 days of accepting a referral and commencing the initial review of a Transaction. One commenter suggested that transactions should be deemed approved if the Secretary does not reach an Initial Determination or Final Determination within a fixed period, with the option for extensions under narrow and defined circumstances. This approach, the commenter argued, would reduce uncertainty for parties to an ICTS Transaction and avoid costly delays. Other commenters asserted that the 180-day limit was too long, given the fast pace of many commercial transactions.

After careful consideration, the Department believes that maintaining the interim final rule's 180-day time limit to issue a Final Determination strikes an appropriate balance between reducing potentially costly delays and ensuring the Department has sufficient time to thoroughly review ICTS Transactions. Notably, to date the Department has not delayed or sought to delay any ICTS Transactions during the pendency of an investigation. However, the Department agrees with commenters that the timeline for reviews was unclear and could create confusion because, among other things, the IFR did not specify when a review is initiated. To improve clarity, this final rule revises the 180-day time limit so that it begins when a party or parties to a transaction are served a copy of an Initial Determination pursuant to § 791.105(b)(3) and grants the Secretary sole discretion to extend this timeline.

Some commenters also requested that the Department implement a formal appeal process following issuance of a Final Determination or a mechanism to allow parties to seek reconsideration based on a change in circumstances. As discussed in the preamble to the IFR, the Department continues to believe that an administrative appeals process is unnecessary in this final rule. The Department directly engages with each party to the ICTS Transaction under review concerning the Department's finding that the party has engaged in a Covered ICTS Transaction, the Department's risk assessment, and whether the Department has initially determined that an ICTS Transaction is prohibited or permitted subject to the adoption of mitigation measures, as described in § 791.107. Each party has an opportunity to respond to the Initial Determination pursuant to § 791.107, including by asserting that there is an insufficient factual or legal basis for the Initial Determination. The Department carefully considers each party's arguments, evidence, or proposed remedial steps prior to making a Final Determination. The Department agrees that reconsideration of a Final Determination may be warranted in some cases, such as if there is a change of circumstances that materially alters the prior assessment. Section 791.6, which remains unchanged from the IFR, permits the Secretary to reconsider Final Determinations unless otherwise provided by law.

This final rule also revises § 791.109(c) in response to a comment which pointed out that the IFR implied that the Secretary has discretion to direct prohibitions that are more restrictive than necessary to address the undue or unacceptable risk resulting from an ICTS Transaction because of the IFR text saying the Secretary has ''*discretion* to direct the least restrictive means necessary to tailor the prohibition to address the undue or unacceptable risk.'' The Department notes that, in most cases, what amounts to the least restrictive means to fully address the risks posed by a Covered ICTS Transaction could be open to different interpretations. Accordingly, this final rule revises § 791.109(c) to clarify that the Secretary will direct the means that the Secretary determines to be necessary to address the undue or unacceptable risk posed by the Covered ICTS Transaction. E.O. 13873 does not require the Secretary to implement the least restrictive means to address undue or unacceptable risk; it provides the Secretary certain discretion to craft mitigation measures that address the overall undue or unacceptable risks posed by ICTS Transactions or classes of ICTS Transactions.

This final rule also amends § 791.109(a) to provide that the Secretary must issue a Final Determination when the Secretary has previously issued an Initial Determination. The interim final rule required a Final Determination only following an Initial Determination that proposed to prohibit an ICTS Transaction. The Department believes that it is important to issue a Final Determination if it has issued an Initial Determination, regardless of whether the Initial Determination proposed to prohibit the ICTS Transaction or permit the ICTS Transaction with mitigation measures, to describe potential risks the Department has identified in connection with an ICTS Transaction, provide a record of decisions, and explain any changes from an Initial Determination.

In addition, this rule includes a new paragraph (9) to § 791.109(d) to clarify that, in cases where the Secretary determines to permit an ICTS Transaction subject to the implementation of measures to mitigate undue or unacceptable risk, the transaction may subsequently be prohibited if a party fails to comply with the terms or obligations of a mitigation agreement. This is not a substantive change from the IFR, but a clarification. Specific criteria for violations that would lead to prohibiting a previously mitigated transaction would be covered in the individual mitigation agreements implemented following the review of an ICTS Transaction or class of ICTS Transactions.

Finally, this action revises § 791.109(f) to clarify that the Secretary publishes notices of Final Determinations in the **Federal Register**, whereas under the IFR the Secretary published the results of Final Determinations to prohibit an ICTS Transaction in the **Federal Register**. This change more accurately represents the intention to publish the outcome of the determination proceedings, without necessarily sharing extensive details about those proceedings. The decision on whether to publish a notice of a Final Determination will vary based on the following new requirements.

The final rule continues to require publication of any Final Determination to prohibit an ICTS Transaction, but as a notice in the **Federal Register**. Publishing a notice of a Final Determination—especially in the case of a determination that a transaction will be prohibited—provides notice to persons about any steps they can take to reduce the risk associated with the ICTS Transaction or to comply with the Final Determination. Additionally, in some cases, the Department may need to inform members of the public about a Final Determination to mitigate risks with the parties to a transaction even if an ICTS Transaction is not prohibited. In those cases, the Secretary may publish a **Federal Register** notice of its Final Determination to mitigate the risk of an ICTS Transaction. Also, if the Department were to issue a **Federal Register** notice about its Initial Determination, the Department will also publish a notice of its Final Determination to inform the public of the Department's final decision to prohibit, mitigate, or permit an ICTS Transaction. In some cases, publication of notices of Final Determinations to prohibit, mitigate, or allow an ICTS Transaction may be valuable to warn the public about identified undue or unacceptable risks or to provide guidance to persons contemplating similar ICTS Transactions. Publication of a Final Determination in the **Federal Register** also provides notice of the Final Determination to persons that are not a party to an ICTS Transaction and who may also be subject to a prohibition in a Final Determination. This final rule also retains the protections for confidential information discussed above, and any published notice of a Final Determination will omit confidential business information under § 791.109(f).

Section 791.200—Penalties

The Department received a few comments on the penalty provisions of § 791.200. Citing the nuances of subcontracting government contracts, some commenters requested that the rule employ an intentionality standard for any violations of the regulation that lead to civil penalties. These commenters argued that the current standard, especially regarding the authorization of penalties for causing any knowing violation, risks confusion and higher compliance costs for contractors with multiple layers of subcontractors. Another commenter suggested that only the parties to a transaction should be held liable for a violation of a Final Determination.

It is possible for a non-party to an ICTS Transaction reviewed by the Department to engage in activities that are contrary to a Final Determination to prohibit an ICTS Transaction, and for those persons to be held liable for violating a prohibition on an ICTS Transaction and therefore these regulations. Also, a person or entity does not need to be a party to an ICTS Transaction to have notice that certain activity is prohibited and to assist or seek to assist others to violate a Final Determination to prohibit an ICTS Transaction (such as by attempting to import a prohibited ICTS) or a Final Determination to mitigate the risk of an ICTS Transaction (for example, directing a party to a mitigation agreement to procure ICTS that does not comply with a mitigation agreement with knowledge that such a mitigation agreement exists). Generally, persons must comply with direction that the Department publishes in the **Federal Register** with regards to mitigating undue or unacceptable risk posed by foreign adversary-nexus ICTS Transactions. The purpose of these rules and of E.O. 13873 is to protect against risks to the ICTS supply chain. In that regard, the penalty provisions serve to encourage U.S. entities engaging in ICTS Transactions with entities with a nexus to a foreign adversary to conduct appropriate due diligence about those transactions or face potential liability.

Although this final rule continues to authorize penalties against persons who are not parties to a transaction, the Department has revised § 791.200 to address commenter concerns about the mental state requirement for a civil violation in certain instances as described in § 791.200(a). Under this final rule, persons can be held responsible for assisting a violation of a Final Determination to mitigate an ICTS Transaction through a mitigation agreement between the U.S. Government and identified parties to an ICTS Transaction, if they have knowledge (as defined at 15 CFR 772.1) that such a mitigation agreement exists. Activities that are prohibited for those with knowledge of the existence of a mitigation agreement includes aiding and abetting violations, commanding a violation, procuring a product that is violative, and other prohibited activities. Finally, providing false information to the Department in connection with an ICTS Transaction under review is also prohibited.

This final rule also amends § 791.200 to clarify the conduct that may lead to penalties under the rule. Section 791.200(a) now provides a list of activities that may lead to civil or criminal penalties under the rule. This list provides more clarity and certainty about prohibited conduct. Section 791.200(b) adds references to the new list of prohibited activities in § 791.200(a) and consolidates and removes duplicative provisions covering civil penalties.

Other Comments

The Department received other comments, discussed below, that were not germane to the rulemaking and outside the scope of this action, or that, for the reasons explained below, the Department does not otherwise address in this final rule.

First, many commenters requested that the Department develop a variety of processes to provide stakeholders with licenses, and guidance about specific transactions that would not be subject to review, or ''pre-clearance,'' before commencing ICTS Transactions. Commenters explained that these processes would provide more certainty to businesses so that they can proactively develop compliance programs and avoid high-risk transactions. Several commenters addressed the potential licensing mechanism that the Department discussed in the preamble to the IFR, but without suggesting a framework for applying for or receiving licenses. Most commenters were in favor of a licensing process, either for parties to seek pre-approval of individual ICTS Transactions, or to exempt all transactions by vetted ICTS manufacturers or suppliers for a fixed period. These commenters stressed, however, that any licensing process should be entirely voluntary and non-duplicative of licensing regimes established by other regulations and should not unnecessarily delay contemplated transactions. Similarly, some commenters requested that the Department establish a list of restricted persons like the Entity List (Supplement No. 4 to Part 744 of the Export Administration Regulations) (15 CFR part 744. Supp.) or develop categories of

transactions that could receive a presumption of approval or denial.

More generally, commenters sought the creation of additional avenues for the Department to provide guidance about the application of the rule. For example, one commenter requested that the Department issue enforcement guidelines and create a mechanism for entities to voluntarily disclose potential violations, while other commenters requested that the Department create a process to issue advisory opinions at the request of entities contemplating ICTS Transactions.

Given the complexity of the issues, the Department appreciates commenters' thoughtful suggestions. The Department is still considering the concepts related to providing licenses, but this final rule does not include a licensing process. Additionally, while the Department anticipates that published Final Determinations will provide guidance to the public about applications of this final rule, the Department understands that additional guidance materials may be useful to those planning compliance with this rule. However, developing procedures to issue guidance or for parties to obtain advisory opinions is outside the scope of this rulemaking, and the Department will seek further comment prior to implementing any rule on that topic.

Second, several commenters asserted that the IFR generally lacked transparency and suggested a number of ways that the Department could assist industry with the interpretation and application of the interim final rule and provide context for the reviews it undertakes. For example, several commenters suggested creating ongoing opportunities for direct industry consultation and engagement such as by hosting industry roundtables. Other commenters suggested that the Department provide an avenue for formal industry comments on reviews before the Secretary issues a Final Determination. Taking a contrary view, other commenters expressed concerns about potential anti-competitive behavior that could result from consultation with industry. The Department appreciates these comments and commenters' willingness to engage with the Department on implementing this rule, but the Department is not adopting any formal avenues for industry and stakeholder engagement in this rule at this time.

IV. Classification

A. Executive Order 12866 (Regulatory Policies and Procedures)

This final rule has been determined to be a ''significant regulatory action'' under section 3(f)(1) of Executive Order 12866, as amended by Executive Order 14094. The Department has examined the expected impact of this final rule as required by those Executive Orders and has conducted a regulatory impact analysis (RIA).

B. Regulatory Flexibility Analysis

The Department has examined the economic implications of this final rule on small entities as required by the Regulatory Flexibility Act (RFA) (5 U.S.C. 601 *et seq.*). The RFA requires an agency to describe the impact of a rule on small entities by providing a regulatory flexibility analysis. The Department published an initial regulatory flexibility analysis in the proposed rule issued on November 27, 2019 (84 FR 65316), published a final regulatory flexibility analysis (FRFA) for the interim final rule (86 FR 4909), and has posted an updated FRFA as part of the RIA for this final rule (see **ADDRESSES** above). The revised FRFA incorporates more recent datasets that have been published since the Department issued the interim final rule and updates the economic analysis to conform to the provisions in the final rule. A summary of the FRFA follows. The Department assesses that the changes in this final rule, relative to the interim final rule, will have a limited economic impact.

Statement of the Objectives of, and Legal Basis for, the Final Rule

A description of this final rule, why it is being implemented, the legal basis, and the purpose of this final rule are contained in the **SUMMARY** and **SUPPLEMENTARY INFORMATION** sections of this preamble, in the preamble to the Notice of Proposed Rulemaking issued on November 27, 2019, and in the preamble to the Interim Final Rule issued on January 19, 2021 (86 FR 4909) and are not repeated here.

A Statement of the Significant Issues Raised by Public Comments or by the Chief Counsel for Advocacy of the Small Business Administration in Response to the FRFA, a Statement of the Assessment of the Agency of Such Issues, and a Statement of Any Changes Made to the Rule as a Result of Such Comments

Many commenters discussed the possibility that this rule would impose significant costs, both on businesses that need to develop compliance plans and on the U.S. economy generally due to the rule's potential effect on corporate profits and viability. Commenters remarked on the RIA's wide range of estimated affected entities and cost to the U.S. economy but questioned whether the RIA included the full range of potential costs or adequately quantified the rule's benefits.

In particular, one commenter noted that the RIA identified, but did not quantify, the cost of the following potential harms: the restriction of imports from adversarial nations, which could increase production costs for many firms; the potential loss of producer profits and lower profits for persons in an industry impacted by a prohibition or mitigation of an ICTS Transaction; the possibility that those who do not engage in transactions affected by the rule may still face higher production costs; the impacts of the rule are not confined to the firms in the industries that produce the products subject to the rule; investors will likely take extra time to evaluate potential transactions, which could result in delays and impose costs on consumers; and higher prices and lower consumer and producer surplus that could arise among inter-related industries. Commenters also critiqued the RIA's failure to quantify the rule's expected benefits to national security and asked for examples of the types of transactions the rule is meant to address to demonstrate its anticipated benefits more clearly and provide a point of reference for the rule's potential scope.

The Department understands commenters' desire for greater certainty in the calculations of the rule's potential costs and benefits. The unquantified harms discussed in the RIA to the interim final rule and listed by a commenter were meant to transparently identify potential downstream effects of the rule. These are not direct costs imposed by the rule and, due to the uncertainty regarding the extent to which they might arise, if at all, the portion of such costs attributable to the rule cannot reasonably be quantified. None of the commenters identified data sources or methods that the Department could use to concretely estimate these costs. As a result, the Department is not changing its earlier analysis of these potential harms.

Regarding the potential benefits of the rule, as discussed in the **SUMMARY** and **SUPPLEMENTARY INFORMATION** sections of this preamble, two years of experience with the interim final rule has shown that the Department's reviews are primarily reviews of classes of transactions involving all or a subset of

all ICTS provided by a single person rather than individual transactions involving a single product or service. As a result, the Department anticipates that such reviews will have a greater impact on national security than would reviews of individual transactions, despite being more limited in number. The Department continues to assess that the actual benefits of this rule are incalculable because it is not possible to predict the type and extent of malicious actions that will be directed at the ICTS supply chain. Moreover, the Department is not providing examples of the types of transactions the rule is meant to address, as requested by commenters. The Department's experience to date has shown that ICTS Transactions present unique risks that would be difficult to describe in generic terms.

Additionally, two commenters asked the Department about the rule's potential impact on commercial items. These commenters asked whether commercial items are exempted from the rule and whether the Secretary has authority over all ICTS, even those with no impact on national security. As discussed in further detail below, the Department considered as an alternative to the rule whether to exclude ICTS Transactions that involve only the acquisition of commercial products as defined by Federal Acquisition Regulation Part 2.101. The Department decided against adopting this alternative to avoid creating an avenue that malicious actors could use to evade the rule. That said, the Secretary's reviews are targeted to ICTS Transactions or classes of Transactions that pose undue risks of sabotage or subversion to the ICTS supply chain and U.S. critical infrastructure or an unacceptable risk to the national security of the United States or the security and safety of U.S. persons. As such, the Department intends to devote its resources to reviewing ICTS Transactions with a potentially negative impact on national security. The Department's modifications to § 791.103 in the final rule to clarify the process that the Secretary will follow to determine which ICTS Transactions are within the scope of the rule are responsive to these comments.

A Description and, Where Feasible, Estimate of the Number of Small Entities to Which the Final Rule Applies

Small Business Administration (SBA) size standards for businesses are based on annual receipts and average employment. For this analysis, as for the analysis for the interim final rule, we define a small business as one employing fewer than 500 persons. This definition allows us to use Census data on firm employment by NAICS industry to estimate the number of affected small entities.

In the RIA, the Department identified 4,533,000 firms in industries that imported significant amounts of goods and services potentially subject to review under the Rule. This formed our upper bound estimate for the total number of affected entities. By replicating this methodology with firm employment data, the Department finds that 4,516,000 of these firms, about 99.6 percent, have fewer than 500 employees. Assuming the lower bound estimate of 268,000 affected entities is also made up of 99.6 percent small businesses, the Department estimates that between 266,995 and 4,516,000 small businesses will be potentially affected by this Rule. The Department's estimate of the number of potentially affected small businesses remains unchanged from the interim final rule.

Federal Rules That May Duplicate, Overlap or Conflict With the Final Rule

The Department did not identify any Federal rule that duplicates, overlaps, or conflicts with this final rule.

Description and Estimate of Economic Effects on Entities, by Entity Size and Industry

In the Costs section of the RIA, the Department estimates that costs to all affected entities will range between approximately $238 million and $20.3 billion (annualized at 7%), or about $2,800 to $6,300 per entity. The Department estimated the costs to small entities using the same methodology, adjusting for changes in hourly wages of operations managers and lawyers over time. As a result of these adjustments, the Department estimates that costs to affected small entities will range between approximately $112 million and $11.1 billion, or about $1,800 and $4,000 per small entity.

Potential Economic Impact of the Rule on Small Entities

Small businesses, as opposed to larger firms, may not have the same ability to deal with the burdens, both direct and indirect, associated with the final rule. Faced with the various costs associated with compliance, firms will have to absorb those costs and/or pass them along to their consumers in the form of higher prices. Either action will reduce the profits of firms. Due to their lack of market power, and their lower profit margins, small firms may find it difficult to pursue either or both of those responses while remaining viable.

A similar situation will hold with respect to the indirect impacts of the final rule. Small firms downstream of impacted industries are likely to face increases in the prices of ICTS they use as inputs and either absorb the increase in cost and/or raise their prices. Given this situation, it is possible that the final rule will have a more substantial adverse impact on small firms relative to larger firms.

However, most of the changes in the final rule, relative to the interim final rule, affect the Department's internal procedures when implementing the rule and will have little impact on small businesses or the broader public. Additionally, many of the changes made from the interim final rule further clarify the scope of ICTS Transactions that the Department may review. These changes may benefit small businesses by reducing uncertainty and, therefore, compliance costs. For example, adding definitions for the terms used in the definition of ''ICTS Transaction'' and specifying who may be considered a ''party or parties to a transaction'' that will receive notice of, and an opportunity to respond to, an Initial Determination, may reduce the cost of learning about the final rule by making it easier to understand which entities and transactions are within the rule's scope.

Similarly, removing the requirement that certain ICTS needs to be in use by at least one million persons to be considered ICTS for purposes of the rule will not specifically increase costs to small entities. While eliminating this threshold means more ICTS Transactions could meet the criteria for review, as noted above, the reality is that most transactions reviewed involve the ICTS from one entity, so removal of the threshold will not increase the number of ICTS Transactions the Department reviews. It might, however, reduce the risk (and associated costs) of U.S. companies feeling pressure to track sales counts of ICTS they suspect or know to be connected to foreign adversaries. Again, the Department is removing the threshold not because the Department intends to or seeks to review more ICTS Transactions by small entities, but rather to indicate to the public that the risks associated with ICTS Transactions are not always related to the volume of or number of people involved in such transactions. The Department's reviews focus on risk posed by foreign adversaries and the ICTS involved.

The Department is also implementing changes to facilitate parties' responses to the Secretary's Initial Determination following an ICTS Transaction review

by, for example, explaining the factual basis supporting the Secretary's Initial Determination. Finally, the Secretary is retaining discretion to publish notices of Final Determinations in the **Federal Register** after determining to prohibit or permit an ICTS Transaction with mitigation measures. The Department's publication of notices of certain Final Determinations enables small business to determine whether their ICTS Transactions are substantially similar to those that have been prohibited or to assess, based on published mitigations, whether they can proactively take any steps to reduce the risks potentially associated with the ICTS Transactions in which they engage.

A Description of, and an Explanation of the Basis for, Assumptions Used

SBA size standards for businesses are based on annual receipts and average employment. For the purpose of this analysis, the Department defines a small business as one employing fewer than 500 persons. This definition allows the Department to use recent Census data on firm employment by NAICS industry to estimate the number of affected small entities. The Department does not have access to sufficiently detailed data on firm employment and receipts to make use of the full set of SBA size standard thresholds.

The Department notes, however, that 84% of SBA employee thresholds are above 500, and 91% of SBA receipt thresholds are above $6 million. Census data show that average receipts for firms employing fewer than 500 employees are $2.2 million. Thus, using our threshold of 500 employees we estimate that about 99.6% of affected entities are small businesses.

Description of Any Significant Alternatives to the Final Rule That Accomplish the Stated Objectives of Applicable Statutes and That Minimize Any Significant Economic Impact of the Rule on Small Entities

This final rule allows the Secretary to review ICTS Transactions to determine whether they present an undue or unacceptable risk to national security, a function which is currently not performed by any other private or public entity. Private industry often lacks the incentive, information, or resources to review their ICTS purchases for malicious suppliers or other potentially bad actors in the ICTS supply chain. The U.S. Government is uniquely situated to determine threats and protect national security, including economic security.

The Department considered two regulatory alternatives to reduce the burden on small entities: (1) excluding small entities with 5 or fewer employees, and (2) excluding certain industries and sectors. However, the Department determined that neither of these alternatives would achieve the goal of protecting national security, nor would they eliminate the Rule's significant economic impact on a substantial number of small entities.

- *No-action alternative:* Rescinding the interim final rule and, accordingly, not implementing a rule under the E.O. is not a viable alternative because E.O. 13873 expressly directs that the Secretary ''shall publish rules or regulations implementing the authorities delegated to the Secretary by this order,'' to address the national security concerns associated with ICTS Transactions in the United States involving foreign adversaries that may create or exploit vulnerabilities in ICTS.
- *Alternative that would categorically exclude small entities or groups of small entities:* The Department considered providing an exemption for small entities that have 5 or fewer employees (smallest entities). According to Census Bureau data, about 6 in 10 employer firms have fewer than 5 employees. The Department also examined the feasibility of eliminating the application of the rule to certain small entities involved in specific industries or sectors by excluding: (a) ICTS Transactions that involve only the acquisition of commercial products as defined by Federal Acquisition Regulation Part 2.101; (b) ICTS Transactions that are used solely for the purpose of cybersecurity mitigation or legitimate cybersecurity research; or (c) ICTS Transactions under which a U.S. person is subject to a security control agreement, special security agreement, or proxy agreement approved by a cognizant security agency to offset foreign ownership, control, or influence pursuant to the National Industrial Security Program regulations (32 CFR part 2004). Ultimately, the Department decided against adopting these regulatory alternatives. Exempting certain industries or sectors or eliminating the application of the final rule to smallest entities could inadvertently allow potentially problematic transactions that are substantially similar to those conducted by non-exempt entities to avoid review, undermining the national security objectives of E.O. 13873. For example, a company that is headquartered in a foreign adversary country, regardless of its size or main industry sector, may be involved in legitimate cybersecurity research and development initiatives performed under the National Cooperative Research and Production Act (15 U.S.C. 4301–06) and the foreign company may study foreign equipment to gain insights on new innovations or potential network security risks. However, that same company may also be conducting operations during other ICTS Transactions that could harm U.S. national security interests. By promulgating the chosen alternative for the rule, the Department sought to remove both the possibility for confusion as well as the ability for malicious actors to argue that some legitimate cybersecurity research performed by a company would exempt all cybersecurity research by a company, legitimate or otherwise. Thus, the rule applies to types of ICTS Transactions most affecting U.S. national security and does not exempt categories of industries, sectors, or entities from review.
- *Preferred alternative:* The final rule is the preferred alternative. It would achieve the objectives of E.O. 13873 by implementing procedures that will allow the Secretary to apply a case-by-case, fact-specific review of ICTS Transactions or classes of Transactions that may pose an undue or unacceptable risk to U.S. national security, critical infrastructure, or U.S. persons and address any identified risks by prohibiting transactions or requiring the implementation of mitigation measures.

Section 212 of the Small Business Regulatory Enforcement Fairness Act of 1996 states that, for each rule or group of related rules for which an agency is required to prepare a FRFA, the agency shall publish one or more guides to assist small entities in complying with the rule and shall designate such publications as ''small entity compliance guides.'' The Department shall explain the actions a small entity is required to take to comply with a rule or group of rules.

C. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) (PRA) provides that an agency generally cannot conduct or sponsor a collection of information, and no person is required to respond to nor be subject to a penalty for failure to comply with a collection of information, unless that collection has obtained Office of Management and Budget (OMB) approval and displays a currently valid OMB Control Number. This final rule does not contain a collection of information requirement subject to review and approval by OMB under the PRA.

D. Unfunded Mandates Reform Act of 1995

This rule would not create a Federal mandate (under the regulatory provisions of Title II of the Unfunded Mandates Reform Act of 1995) for State, local, and tribal governments or the private sector.

E. Executive Order 13132 (Federalism)

This rule does not contain policies having federalism implications requiring preparations of a Federalism Summary Impact Statement.

F. Executive Order 12630 (Governmental Actions and Interference With Constitutionally Protected Property Rights)

This rule does not contain policies that have unconstitutional takings implications.

G. Executive Order 13175 (Consultation and Coordination With Indian Tribes)

The Department has analyzed this rule under Executive Order 13175 and has determined that the action would not have a substantial direct effect on one or more Indian tribes, would not impose substantial direct compliance costs on Indian tribal governments, and would not preempt tribal law.

H. National Environmental Policy Act

The Department has reviewed this rulemaking action for the purposes of the National Environmental Policy Act (42 U.S.C. 4321 *et seq.*). It has determined that this final rule would not have a significant impact on the quality of the human environment.

I. Congressional Review Act

This rule has been determined to be a ''major rule'' under the Congressional Review Act (5 U.S.C. 801 *et seq.*).

List of Subjects in 15 CFR Part 791

Administrative practice and procedure, Business and industry, Communications, Computer technology, Critical infrastructure, Executive orders, Foreign persons, Investigations, National security, Penalties, Technology, Telecommunications.

For the reasons stated in the preamble, the Department amends 15 CFR part 791 as follows:

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

■ 1. The authority citation for 15 CFR Part 791 continues to read as follows:

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.

■ 2. In Part 791, remove the text ''initial determination'' wherever it appears, and add, in its place, the text ''Initial Determination''.

■ 3. In Part 791, remove the text ''final determination'' wherever it appears, and add, in its place, the text ''Final Determination''.

■ 4. Amend § 791.1 by revising paragraph (a)(1) to read 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;

* * * * *

■ 5. Amend § 791.2 by:

■ a. Revising the definition of ''Appropriate agency heads'';

■ b, Adding in alphabetical order definitions for ''Covered ICTS Transaction'', ''Dealing in'', and ''Importation'';

■ c. 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''.

The additions and revisions read 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.

* * * * *

■ 6. Amend § 791.3 by revising paragraphs (a)(2), (4) and (b), and removing paragraph (c), to read as follows:

§ 791.3 Scope of Covered ICTS Transactions.

(a) The Secretary may continue review under § 791.103(b) of this part for any ICTS Transaction that:

* * * * *

(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.

■ 7. Amend § 791.4 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) to read 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.

■ 8. Amend § 791.100 by revising paragraph (a) introductory text, (a)(6), (7), (8), and (9), paragraph (c) introductory text, paragraph (d) introductory text, (d)(5), and (e) to read 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.

■ 9. Revise paragraphs (a) and (b) of § 791.101 to read 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.

* * * * *

■ 10. Amend § 791.102 by revising the introductory text of paragraph (b), (b)(4) through (6), and adding (b)(7) to read 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.

* * * * *

■ 11. Revise § 791.103 to read 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.

■ 12. Revise § 791.104 to read 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.

■ 13. Revise § 791.105 to read 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**.

■ 14. Revise § 791.106 to read 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.

■ 15. Amend § 791.107 by revising the introductory text, paragraphs (c), (e), (f) to read 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.

■ 16. Revise § 791.108 to read 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.

■ 17. Revise § 791.109 to read 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.

■ 18. Revise § 791.200 to read as follows:

§ 791.200 Penalties.

(a) *Prohibited activities.* (1) No person shall be a party to an ICTS Transaction that is prohibited by a Final Determination issued under this part, unless authorized by the Secretary.

(2) No person shall aid, abet, counsel, command, induce, facilitate, procure, or otherwise engage in conduct with knowledge that such conduct is prohibited by, or contrary to a Final Determination issued under this part, unless authorized by the Secretary.

(3) No person shall be a party to an ICTS Transaction in a manner that is contrary to any direction, regulation, or condition published under this part.

(4) No person shall aid, abet, counsel, command, induce, facilitate, procure, or otherwise engage in conduct with knowledge that such conduct is contrary to the terms of a mitigation agreement under this part.

(5) Any ICTS Transaction that has the purpose of evading or avoiding, causes a violation of, or attempts to violate, any of the prohibitions set forth in this section is prohibited.

(6) Any conspiracy formed to violate any of the prohibitions set forth in this section is prohibited.

(7) Any approval, financing, facilitation, or guarantee by a United States person, wherever located, of an ICTS Transaction by a foreign person where the ICTS Transaction by that foreign person would be prohibited by this order if performed by a United States person or within the United States, is prohibited.

(8) No person may, whether directly or indirectly through any other person, make any false or misleading representation, statement, or certification, or falsify or conceal any material fact, to the Department:

(i) In the course of an ICTS Transaction review, in order to secure a benefit or avoid a prohibition, including in proposing and agreeing to mitigation measures; or

(ii) In connection with the preparation, submission, issuance, use, or maintenance of any report filed or required to be filed pursuant to this part.

(9) Additional requirements:

(i) For purposes of paragraph (a)(8), any representation, statement, or certification made by any person shall be deemed to be continuing in effect until the person notifies the Department in accordance with paragraph (a)(9)(ii).

(ii) Any person who makes a representation, statement, or certification to the Department relating to any ICTS Transaction review shall notify the Department, in writing, of any change of any material fact or intention from that previously represented, stated, or certified, immediately upon receipt of any information that would lead a reasonably prudent person to know that a change of material fact or intention had occurred or may occur in the future.

(b) *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 paragraph (a) of this section. IEEPA provides for a maximum civil penalty not to exceed the greater of $250,000 per violation, 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.

(i) Notice of the penalty, including a written explanation of the penalized conduct specifying the laws and regulations allegedly violated and the amount of the proposed penalty, and notifying the recipient of a right to make a written petition within 30 days as to why a penalty should not be imposed, shall be served on the person.

(ii) The Secretary shall review any presentation and issue a final administrative decision within 30 days of receipt of the petition.

(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 paragraph (a) of this section shall, upon conviction of a violation of IEEPA, be fined not more than $1,000,000, or if a natural person, may be imprisoned for not more than 20 years, or both.

(3) Any civil penalties authorized in this section may be recovered in a civil action brought by the United States in U.S. district court.

(c) *Adjustments to penalty amounts.* (1) The civil penalties provided in IEEPA are subject to adjustment pursuant to the Federal Civil Penalties Inflation Adjustment Act of 1990 (Pub. L. 101–410, as amended, 28 U.S.C. 2461 note).

(2) The criminal penalties provided in IEEPA are subject to adjustment pursuant to 18 U.S.C. 3571.

(d) *Available penalties.* The penalties available under this section are without prejudice to other penalties, civil or criminal, available under law. Attention is directed to 18 U.S.C. 1001, which provides that whoever, in any matter within the jurisdiction of any department or agency in the United States, knowingly and willfully falsifies, conceals, or covers up by any trick, scheme, or device a material fact, or makes any false, fictitious, or fraudulent statements or representations, or makes or uses any false writing or document knowing the same to contain any false, fictitious, or fraudulent statement or entry, shall be fined under title 18, United States Code, or imprisoned not more than 5 years, or both.

Elizabeth L.D. Cannon,

Executive Director, Office of Information and Communications Technology and Services.

[FR Doc. 2024–28335 Filed 12–5–24; 8:45 am]

BILLING CODE 3510–20–P

COMMODITY FUTURES TRADING COMMISSION

17 CFR Part 40

RIN 3038–AF28

Provisions Common to Registered Entities; Correction

AGENCY: Commodity Futures Trading Commission.

ACTION: Final rule; correction.

SUMMARY: The Commodity Futures Trading Commission (Commission) is correcting a final rule that appeared in the **Federal Register** on November 7, 2024. The document clarified, simplified and enhanced the utility of certain regulations for registered entities, market participants and the Commission that govern how registered entities submit self-certifications, and requests for approval, of their rules, rule amendments, and new products for trading and clearing, as well as the Commission's review and processing of such submissions.

DATES: Effective December 9, 2024.

FOR FURTHER INFORMATION CONTACT: Rachel Kaplan, Senior Special Counsel, *rkaplan@cftc.gov,* 202–418–6233, Steven Benton, Industry Economist, *sbenton@cftc.gov,* 202–418–5617, and Nancy Markowitz, Deputy Director, *nmarkowitz@cftc.gov,* 202–418–5453, Division of Market Oversight, and Eileen Chotiner, Senior Compliance Analyst, *echotiner@cftc.gov,* 202–418–5467, Division of Clearing and Risk, Commodity Futures Trading Commission, Three Lafayette Centre, 1151 21st Street NW, Washington, DC 20581.

SUPPLEMENTARY INFORMATION: In FR Doc. 2024–24388 appearing on page 88594 in the **Federal Register** of Thursday, November 7, 2024, the following corrections are made:

§ 40.2 [Corrected]

■ 1. On page 88623 in the second column, in § 40.2, before the first sentence in paragraph (a) introductory text, add the paragraph heading ''*Submission requirements.*''.

§ 40.5 [Corrected]

■ 2. On page 88625 in the first column, in § 40.5, in amendment 9h, the instruction ''Revising paragraph (d) introductory text and (d)(1);'' is corrected to read ''Revising paragraph (d) introductory text and adding new paragraph (d)(1);''

■ 3. On page 88625 in the second column, in § 40.5, in amendment 9m, the instruction ''Redesignating paragraphs (f)(1) and (2) as paragraphs (e)(1) and (2) respectively; and'' is corrected to read ''Redesignating paragraph (f) as paragraph (e) and revising newly redesignated paragraph (e); and''

■ 4. On page 88625 in the second column, in § 40.5, remove amendment 9n.

■ 5. On page 88625 in the third column, in § 40.5, ''(c) * * *'' is corrected to read ''(c) *Commission review.*''.