: 3510-20-P

DEPARTMENT OF COMMERCE

15 CFR Part 7

[Docket No. 210113-0009]

RIN 0605-AA51

Securing the Information and Communications Technology and Services Supply Chain

AGENCY: U.S. Department of Commerce.

ACTION: Interim final rule; request for comments.

SUMMARY: The Department of Commerce is promulgating regulations to implement provisions of Executive Order 13873, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain" (May 15, 2019). These regulations create the processes and procedures that the Secretary of Commerce will use to identify, assess, and address certain transactions, including classes of transactions, between U.S. persons and foreign persons that involve information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and pose an undue or unacceptable risk. While this interim final rule will become effective on [Insert date 60 days after publication in the FEDERAL REGISTER], the Department of Commerce continues to welcome public input and is thus seeking additional public comment. Once any additional comments have been evaluated, the Department is committed to issuing a final rule.

DATES: Effective [*insert date 60 days after date of publication in the FEDERAL REGISTER*]. Comments to the interim final rule must be received on or before [Insert date 60 days after publication in the FEDERAL REGISTER].

ADDRESSES: All comments must be submitted by one of the following methods:

- *By the Federal eRulemaking Portal: http://www.regulations.gov* at docket number [DOC-2019-0005].

- *By email directly to: ICTsupplychain@doc.gov.* Include "RIN 0605-AA51" in the subject line.
- *Instructions:* Comments sent by any other method, to any other address or individual, or received after the end of the comment period, may not be considered. For those seeking to submit confidential business information (CBI), please clearly mark such submissions as CBI and submit by email, mail, or hand delivery as instructed above. Each CBI submission must also contain a summary of the CBI, clearly marked as public, in sufficient detail to permit a reasonable understanding of the substance of the information for public consumption. Such summary information will be posted on *regulations.gov.*
- Supporting documents:
    - The Regulatory Impact Analysis is available at http://www.regulations.gov at docket number [DOC-2019-0005];
    - The Center for Strategic & International Studies, "Significant Cyber Incidents 2020" is available at https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents;
    - The National Security Strategy of the United States is available at https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf;
    - ODNI's 2016-2019 Worldwide Threat Assessments of the U.S. Intelligence Community are available at https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf (2017), https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf (2018), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf (2019); and

- The 2018 National Cyber Strategy of the United States of America is available at https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

FOR FURTHER INFORMATION CONTACT: Henry Young, U.S. Department of Commerce, telephone: (202) 482-0224. For media inquiries: Meghan Burris, Director, Office of Public Affairs, U.S. Department of Commerce, telephone: (202) 482-4883.

SUPPLEMENTARY INFORMATION:

I. Background

The information and communications technology and services (ICTS) supply chain is critical to nearly every aspect of U.S. national security. U.S. business and governments at all levels rely heavily on ICTS, which: underpin our economy; support critical infrastructure and emergency services; and facilitate the Nation's ability to store, process, and transmit vast amounts of data, including sensitive information, that is used for personal, commercial, government, and national security purposes. The ICTS supply chain must be secure to protect our national security, including the economic strength that is an essential element of our national security. Ensuring the resilience of, and trust in, our ICTS supply chain is an issue that touches upon national security, including economic security, and public health and safety.

The purchase, incorporation, and use by U.S. persons of ICTS—such as network management or data storage—produced by any person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary – can create multiple opportunities for those foreign adversaries to exploit potential vulnerabilities in the ICTS. That, in turn, could cause direct and indirect harm to both the immediate targets of the adverse action and to the United States as a whole. While attacks can originate from remote foreign sources, incorporating certain software, equipment, and products into U.S. domestic ICTS networks, as well as the use of certain cloud, network management, or other services, greatly increases the risk that potential vulnerabilities may be introduced, or that vulnerabilities may be present without being detected.

These potential vulnerabilities, if exploited, could undermine the confidentiality, integrity, and availability of U.S. person data including personally identifiable information or other sensitive personal data.

Some foreign adversaries are known to exploit the sale of software and hardware to introduce vulnerabilities that can allow them to steal critical intellectual property, research results (e.g., health data), or government or financial information from users of the software or hardware. Such vulnerabilities can be introduced in the network, cloud service, or individual product data; allow traffic monitoring or surveillance; and may be resistant to detection by private purchasers or telecommunications carriers. Once detected, such vulnerabilities may be extremely costly or impossible to remediate.

Vulnerabilities to data integrity can be created by including a foreign adversary's hardware and software into U.S. networks and systems. This incorporated hardware and software poses opportunities to add or remove important information, modify files or data streams, slow down, or otherwise modify the normal transmission or availability of data across U.S. networks. Such capabilities could be exercised in areas as diverse as financial market communications, satellite communications or control, or sensitive consumer information.

A foreign adversary could also exploit vulnerabilities provided by the incorporation of hardware and software into U.S. environments by fully or partially closing down critical networks or functions at key times. These types of attacks are known as denial of service attacks. Such attacks could cause widespread problems, such as if they occur during periods of crisis, or they could be used selectively by targeting individual corporations or important infrastructure elements or functions. They could also be masked to make the source of the disruption difficult to attribute and, therefore, difficult to trace and stop.

These risks are not necessarily confined to infrastructure environments. They could, for example, be present in the use of cloud services, as well as in the widespread use of some consumer devices, networked surveillance cameras, drones, or interconnection via the internet of

computing devices embedded in everyday objects, enabling them to send and receive data. For example, applications ("apps"), which may be downloaded from app stores or web browsers by a user to a mobile device, may automatically capture vast swaths of sensitive personal data from its users, including Internet and other network activity information such as location data and browsing and search histories. This data exfiltration—supported by U.S. web data hosting and storage servers—threatens to allow foreign adversaries to exploit Americans' personal and proprietary information by allowing a foreign adversary to track the locations of Americans, build dossiers of sensitive personal data for blackmail, and conduct corporate espionage from inside the borders of the United States.

Multiple reported cybersecurity incidents in the United States and among major allies in 2020 illustrate the potential risk in permitting unrestricted access to U.S. ICTS supply chains, such as:

- In July 2020, two Chinese hackers working with the Chinese Ministry of State Security were indicted by the U.S. Department of Justice for conducting a global computer intrusion campaign targeting U.S. intellectual property and confidential business information, including COVID-19 vaccine research;
- German officials announced that a Russian hacking group associated with the Federal Security Bureau had compromised the networks of energy, water, and power companies in Germany by exploiting ICTS supply chains; and
- Japan's Defense Ministry announced it was investigating a large-scale cyber attack against Mitsubishi Electric that could have compromised details of new state-of-the-art missile designs.

See, e.g., Center for Strategic & International Studies, "Significant Cyber Incidents 2020," available at https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.

Consequently, the President has determined that the unrestricted acquisition or use of

ICTS that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.

Executive Order 13873 of May 15, 2019, "Securing the Information and Communications Technology and Services Supply Chain" (84 FR 22689) (Executive Order), was issued pursuant to the President's authority under the Constitution and the laws of the United States, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq.*), and section 301 of Title 3, United States Code. IEEPA and the Executive Order grant the Secretary of Commerce (Secretary) the authority to prohibit any acquisition, importation, transfer, installation, dealing in, or use of any ICTS (an "ICTS Transaction") by any person, or with respect to any property, subject to United States jurisdiction, when such ICTS Transaction involves any property in which a foreign country or national has any interest, and the Secretary, in consultation with other agency heads (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 as the Secretary determines is appropriate) determines that the 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; and (2) poses an undue or unacceptable risk. Executive Order, Section 1(a). The Executive Order further provides the Secretary with the authority to prohibit such an ICTS Transaction or "design or negotiate measures to mitigate concerns" about an ICTS Transaction's impact on national security. Executive Order, Section 1(b).

On November 27, 2019, the Department of Commerce (Department) published a proposed rule to implement the terms of the Executive Order. (84 FR 65316). The proposed rule

set forth processes for (1) how the Secretary would evaluate and assess transactions involving ICTS 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) how the Secretary would notify parties to transactions under review of the Secretary's decision regarding the ICTS Transaction, including whether the Secretary would prohibit or mitigate the transaction; and (3) how parties to transactions reviewed by the Secretary could comment on the Secretary's preliminary decisions. The proposed rule also provided that the Secretary could act without complying with the proposed procedures where required by national security. Finally, the Secretary would establish penalties for violations of mitigation agreements, the regulations, or the Executive Order.

In addition to seeking general public comment, the Department requested comments from the public on five specific questions: (1) whether the Secretary should consider categorical exclusions or whether there are classes of persons whose use of ICTS cannot violate the Executive Order; (2) whether there are categories of uses or of risks that are always capable of being reliably and adequately mitigated; (3) how the Secretary should monitor and enforce any mitigation agreements applied to a transaction; (4) how the terms, "transaction," "dealing in," and "use of" should be clarified in the rule; and (5) whether the Department should add record-keeping requirements for information related to transactions.

In response to requests for additional time in which to comment on the proposed rule, the Department extended the initial comment period from December 27, 2019, until January 10, 2020. (84 Fed. Reg. 70445). As reflected herein, the Department has carefully considered and addressed the public's comments in promulgating this rule.

Nonetheless, because several commenters requested that the Department provide for an additional round of public comment, and in an effort to continue the Department's work to protect the national security while reducing the regulatory impact on the public, the Department is taking further public comment on the rule. However, mindful of the urgent need of the United

States to address national security concerns related to ICTS Transactions, this interim final rule will be effective [Insert date 60 days from the date of publication in the FEDERAL REGISTER]. The Department is committed to issuing a subsequent final rule in which the Department will consider and respond to additional comments received. In addition, the Department will implement and publish procedures for a licensing process by [*insert date 120 days from date of publication in the* ***Federal Register***].

II. Response to Comments

During the public comment period on the proposed rule, the Department received a number of written submissions reflecting a wide range of views. All comments received by the end of the comment period are available on the public rulemaking docket at https://www.regulations.gov. Additionally, the Department participated in a number of meetings with foreign governments and industry groups to discuss the proposed rule prior to the comment period ending. Summaries of those meetings are available at https://www.regulations.gov. Below, the Department addresses the comments as they pertain to each relevant provision of the regulation.

§ 7.2 Definitions.

§ 7.2 - Definition of "appropriate agency heads"

Numerous comments addressed the extent to which the Department interacts with other agencies and department heads throughout the process for reviewing ICTS Transactions. Some commenters advocated for the rule to require interagency review of all parts of the investigations and final determinations, while other commenters noted that interagency review should only happen during certain parts of the review process. Other commenters requested that the Secretary notify the heads of relevant agencies when a review is initiated.

Requirements regarding interagency review are already contained within the Executive

Order and, thus, are not subject to change.

Nevertheless, for clarification, the Department has replaced the term "identified secretaries" with "appropriate agency heads," to address the fact that some of the individuals referenced are not Cabinet Secretaries, but rather are heads of agencies. For clarity, the term "appropriate agency heads" refers to 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 of Commerce determines is appropriate. The Executive Order makes clear the Secretary of Commerce will confer with other agencies and departments as needed.

§ 7.2 – Definition of "Department"

Although it was not defined in the proposed rule, the Department has added a definition of the term "Department" to clarify that it refers to the United States Department of Commerce, rather than any other Cabinet-level agency.

§ 7.2 - Definition of "foreign adversary"

The rule grants the Secretary the authority to block or mitigate certain ICTS Transactions involving a foreign adversary. Commenters suggested limiting the definition of a "foreign adversary" to entities already identified in legislation. Some commenters recommended changing the concept of "foreign adversary" to focus on entities or persons instead of nation-states. Other commenters suggested that the Department create a list of adversaries and a list of exempt countries and distinguish between government and non-governmental entities. Commenters also recommended narrowing the scope of the term "foreign adversary" to situations where a foreign adversary has controlling interest in the company executing the covered transaction.

The rule makes no changes to the definition of "foreign adversary," which is consistent with the Executive Order's definition. However, as discussed further below, the rule now includes a provision titled "Determination of foreign adversaries" in section 7.4. This provision sets out the list of foreign governments and foreign non-government persons that the Secretary has determined, solely for the purposes of the Executive Order, this rule, and any subsequent rules, are "foreign adversaries." It also explains some of the factors that the Secretary considered, and will consider, when making any future determinations of whether a country is a "foreign adversary." Pursuant to the Secretary's discretion, the list of foreign adversaries will be revised as determined to be necessary. Because the determination of foreign adversaries is subject solely to the Secretary's discretion, such revisions will be effective immediately upon publication in the Federal Register without prior notice or opportunity for public comment.

The list of "foreign adversaries" consists of the following foreign governments and non-government persons: the People's Republic of China, including the Hong Kong Special Administrative Region (China); the Republic of Cuba (Cuba); the Islamic Republic of Iran (Iran); the Democratic People's Republic of Korea (North Korea); the Russian Federation (Russia); and Venezuelan politician Nicolás Maduro (Maduro Regime). The provision clarifies that the Secretary's determination is based on multiple sources, including the National Security Strategy of the United States, the Office of the Director of National Intelligence's 2016-2019 Worldwide Threat Assessments of the U.S. Intelligence Community, and the 2018 National Cyber Strategy of the United States of America, as well as other reports and assessments from the U.S. Intelligence Community, the U.S. Departments of Justice, State and Homeland Security, and other relevant sources. Additionally, the provision notes that the Secretary will periodically review this list in consultation with appropriate agency heads and may add to, subtract from, supplement, or otherwise amend the list.

It is important to note that the list at section 7.4 identifies "foreign adversaries" solely for the purposes of the Executive Order, this rule, and any subsequent rules. It does not reflect a

determination by the United States about the nature of such foreign governments or foreign non-government persons for any other purpose.

§ 7.2 – Definition of "ICTS Transaction"

The proposed rule defined the term "transaction" using terms from the Executive Order, to mean, "any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service." It also noted that the term "transaction" "includes a class of transactions."

Some commenters requested the Department refine the definition of "transaction" in various ways. For example, some commenters suggested adopting language from the Securities Exchange Act of 1934 to define some of the terms in the definition, such as "dealing in." Others urged the Department to further clarify the definition "transaction" to define the terms "acquisition," or "use" in the definition.

The Department acknowledges that the terms "transaction," "acquisition," and "use" are broad, and retain their commonly-accepted meanings in the rule. The concerns raised by the commenters are addressed by defining the term "ICTS Transaction" to include (1) "ongoing activities, such as managed services, data transmission, software updates, repairs, or the platforming or data hosting of applications for consumer download;" and (2) "any other transaction, the structure of which is designed or intended to evade or circumvent the application of the Executive Order." The purpose of these additions is to clarify that the Secretary may review ICTS Transactions, including the provision of services, that occur on or after [Insert Date of publication in the FEDERAL REGISTER], by any person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. Providing services, such as software updates, to U.S. persons may provide a foreign adversary an opportunity to engage in the types of activities that may threaten U.S. national security, as described above. Further, the definition of ICTS Transaction clarifies that attempting to structure a transaction in order to circumvent

Secretarial review is nonetheless an ICTS Transaction subject to this rule.

§ 7.2 - Definition of "party or parties to a transaction"

Several commenters expressed an interest in the Department further clarifying what entities are covered by the rule. Further, in revising the proposed rule for finalization, the Department used the term "party to a transaction" in several instances and believes it would be beneficial to define that term. Accordingly, the rule adds a definition of "party or parties to a transaction," to mean a person engaged in an ICTS Transaction, including the person acquiring the ICTS and the person from whom the ICTS is acquired. The term "person" is also defined by the rule and is unchanged from the proposed rule.

"Party or parties to a transaction" include entities designed or intended to evade or circumvent application of the Executive Order. For purposes of this rule, this definition does not include common carriers that transport goods for a fee on behalf of the general public, except to the extent that a common carrier knows, or should have known (as the term "knowledge" is defined in 15 CFR 772.1), 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 Department or permitted subject to mitigation measures.

This addition narrows the scope of the rule by adding clarity regarding which persons are responsible for a reviewable transaction. This also affects which parties will be notified by the Department regarding any potential review of a transaction.

§ 7.2 – Definition of "Person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary"

In addition to defining "party or parties to a transaction," the Department sought to add clarity to the rule by defining the phrase "person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary," as many commenters expressed concern that

leaving such terms undefined might create confusion about the breadth of the rule's reach. The Department defines "person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" to mean "any person, wherever located, who acts as an agent, representative, or employee, or any person who acts in any other capacity at the order, request, or under the direction or control, of a foreign adversary or of a person whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized in whole or in majority part by a foreign adversary; any person, wherever located, who is a citizen or resident of a nation-state controlled by a foreign adversary; any corporation, partnership, association, or other organization organized under the laws of a nation-state controlled by a foreign adversary; and any corporation, partnership, association, or other organization, wherever organized or doing business, that is owned or controlled by a foreign adversary."

§ 7.2 – Sensitive Personal Data

Many commenters requested additional clarity about the specific ICTS that is subject to this rule. While it is impossible to identify all of the ICTS that may present undue or unnecessary risks, the Department has defined the term, "sensitive personal data," to identify, along with the information identified in section 7.3 of the rule, some of types of information or communications that might be involved in an ICTS Transaction reviewed under this rule where a party or parties to a transaction use, possess, or retain, or are expected to use, possess, or retain sensitive personal data.

The term "sensitive personal data" includes: (1) Personally Identifiable Information (i.e., data that can identify individuals) that is maintained or collected by a U.S. business operating in specific areas, and that is maintained or collected on over one million people over a 12 month period; and (2) results of individual genetic testing.

The categories of identifiable data of concern to the Department are: financial data that could be used to indicate an individual's financial distress or hardship; the set of data included in

consumer reports; the set of data used for health and certain financial insurance applications; data relating to the physical, mental, or psychological health condition of an individual; non-public electronic communication information, such as personal emails; geolocation data used in certain technologies; biometric data; data stored and processed for generating Federal, State, Tribal, Territorial, or other government identification cards; data concerning U.S. Government personnel security clearance status; and data from security clearance or employment applications.

As indicated in section 7.3, Scope, the Department believes that ICTS Transactions involving sensitive personal data could create risks for the U.S. national security and also believes it is important to specifically identify these categories of data to provide the regulated community with additional specificity and certainty as to the scope of the rule's application.

§ 7.2 - Definition of "Undue or unacceptable risk"

Commenters recommended various alternative uses for and limits on this term. For example, some suggested that the Department identify certain industries or types of transactions that do not pose a risk to national security, and that the Department should exempt certain types of transactions from the rule.

Most of the suggestions could unnecessarily limit the United States' ability to determine its national security interests and, thus, could limit the ability to protect the Nation. However, the Department agrees the term requires definition, and in this rule adopts the definition of "undue or unacceptable risks" as those risks identified in Section 1(a)(ii) of the Executive Order. Section 1(a)(ii) of the Executive Order includes the following risks …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; …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 …an unacceptable

risk to the national security of the United States or the security and safety of United States persons.

§ 7.3 Scope of Covered ICTS Transactions.

Many commenters suggested ways the Department could narrow the scope of the rule to provide more guidance for the types of transactions the Department may review. For example, commenters noted the potential impact of the proposed rule on certain types of transactions, such as transportation services of ICTS, and argued the rule would harm commenters' industries. They also argued that the proposed rule was overly broad and that narrowing the scope would bring greater economic certainty to ICTS Transactions and the technology industry as a whole.

Other commenters sought to have the Department identify categorical exemptions for select industries, such as ICTS Transactions involving medical devices or services for air traffic control, while yet others sought to exempt transactions involving companies with their business headquarters in allied nations, such as Japan. Commenters also suggested that, provided appropriate cybersecurity mitigation techniques exist, transactions involving otherwise banned equipment should be exempted from this rule.

The Department concludes that categorical exemptions of specific industries or geographic locations are unwarranted at this time, although the Secretary may consider this possibility in the future. Wholesale exemptions of industries and geographic locations would not serve the rule's intended purpose of securing the ICTS supply chain because such exemptions would contradict the Department's evaluation method for ICTS Transactions. Such exemptions would indicate to foreign adversaries whole classes of ICTS Transactions outside the scope of evaluation under this rule. This would allow foreign adversaries to pinpoint certain types of ICTS Transactions that would more easily escape Departmental oversight and, therefore, threaten U.S. national security. By retaining broad authority across industries, the Department will be better able to mitigate identified risks.

While the rule does not contain categorical exemptions of specific industries or geographic locations, the rule now specifies that ICTS Transactions that involve certain technologies, hardware, or software will be considered to be covered ICTS Transactions. Additionally, the rule does make clear that, as further discussed below, 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, is not an ICTS Transaction. Additionally, the Department acknowledges that ICTS Transactions solely involving personal ICTS hardware devices, such as handsets, do not warrant particular scrutiny.

§ 7.3 – Technology Sectors

Many commenters requested that the Department identify those technologies or products that the Department considers create the greatest risks to the national security of the United States. The Department understands the desire for additional certainty and broke down the scope of technologies included under the scope of this rule into six main types of ICTS Transactions involving: (1) ICTS that will be used by a party to a transaction in a sector designated as critical infrastructure by Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience, including any subsectors or subsequently designated sectors; (2) software, hardware, or any other product or service integral to wireless local area networks, mobile networks, satellite payloads, satellite operations and control, cable access points, wireline access points, core networking systems, or long- and short-haul systems; (3) software, hardware, or any other product or service integral to data hosting or computing services that uses, processes, or retains, or is expected to use, process, or retain, sensitive personal data on greater than one million U.S. persons at any point over the twelve months preceding an ICTS Transaction; (4) certain ICTS products which greater than one million units have been sold to U.S. persons at any point over the twelve months prior to an ICTS Transaction; (5) software designed primarily for connecting with and communicating via the Internet that is in use by greater than one million U.S. persons at

any point over the twelve months preceding an ICTS Transaction; (6) ICTS integral to artificial intelligence and machine learning, quantum key distribution, quantum computing, drones, autonomous systems, or advanced robotics.

§ 7.3 - Licensing Process for Potential Transactions

Many commenters requested that the Department establish a process for entities to seek pre-approval of their ICTS Transactions, similar to the process by which entities may inform the Committee on Foreign Investment in the United States (CFIUS) of investments in U.S. businesses, and obtain "safe harbor" for those transactions. Commenters argued that such a process would help ease business uncertainty in specific cases.

To afford parties greater certainty, within 60 days of the publication date of this rule, the Department intends to publish procedures to allow a party or parties to a proposed, pending, or ongoing ICTS Transaction to seek a license, pursuant to Section 2(b) of the Executive Order, in a manner consistent with the national security of the United States. Within 120 days of the publication date of this rule, the Department intends to implement this licensing process. The published procedures will establish criteria by which persons may seek a license to enter into a proposed or pending ICTS Transaction or engage in an ongoing ICTS Transaction. Persons who may seek a license will include any parties to a proposed, pending, or ongoing ICTS Transaction as that term is defined in this rule. License application reviews will be conducted on a fixed timeline, not to exceed 120 days from accepting a license application, to enable qualifying parties to conclude permissible transactions without undue delay. If the Department does not issue a license decision within 120 days from accepting a license application, the application will be deemed granted. In no event, however, would the Department issue a license decision on an ICTS Transaction that would reveal sensitive information to foreign adversaries or others who may seek to undermine U.S. national security. Qualifying parties may voluntarily apply for a license, and a party's decision not to seek a license will not create a negative inference or

unfavorable presumption with respect to a transaction.

§ 7.3 - Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience

Regarding the Department's assessment of undue and unacceptable risk, commenters suggested that the Department create risk criticality categories for transactions, such as low, medium, and high, along with different assessment approaches. Other commenters advocated using risk scores or categories to determine the frequency and rigor of monitoring.

The Department agrees that the scope of the rule could be narrowed to indicate more specifically the types of ICTS Transactions that may be reviewed. Accordingly, the Department clarifies that ICTS Transactions include those that involve, among other aspects, a sector designated as critical infrastructure by Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience, including any subsectors or subsequently designated sectors. As explained below, the Department has also clarified that transactions involving certain sensitive personal data, regardless of whether they involve a critical infrastructure sector, will be considered ICTS Transactions for the purposes of the rule.

§ 7.3 Exclusions

Many commenters sought clarity about the relationship of this rule to the rules relating to CFIUS's review of transactions. In response, the Department is clarifying that this rule does not apply to an ICTS Transaction that CFIUS is actively reviewing, or has reviewed, as a covered transaction or covered real estate transaction or as part of such a transaction under section 721 of the Defense Production Act of 1950, as amended, and its implementing regulations. Note, however, that a transaction involving ICTS that is separate from, and subsequent to, a transaction for which CFIUS has concluded action under section 721 may be subject to review under this rule, if and to the extent that such transactions are separate from the transaction reviewed by CFIUS. Parties should therefore be aware that CFIUS review related to a particular ICTS, by

itself, does not present a safe harbor for future transactions involving the same ICTS that may present undue or unnecessary risks as determined by the Department.

§ 7.3 – Exclusions of ICTS Transactions

Commenters requested categorical exclusions across many sectors, industries, functions, and nations. The Secretary recognizes the need to be judicious and deliberate in deciding what types of ICTS Transactions pose an undue or unacceptable risk. To that end, the rule excludes from the scope of the rule those transactions that involve 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, because they are subject to continuous security oversight by, and contractual obligations to, other Federal agencies.

§ 7.3 - Retroactivity of Rule's Applicability

Some commenters argued that the rule should not apply to transactions that took place prior to May 15, 2019, when the Executive Order was issued. Other commenters advocated for the complete elimination of the proposed rule's retroactivity provisions, and proposed the Department only evaluate potential transactions prospectively. Other commenters proposed grandfathering some ICTS equipment for a predetermined duration, potentially up to 10 years. In reviewing these comments and the proposed rule, the Department determined that the temporal limits of the rule's application could be clarified.

In response to these comments, the Department has clarified, in section 7.3(a)(3), that the rule applies to an ICTS Transactions that is initiated, pending, or completed on or after [Date of publication in the FEDERAL REGISTER]. Further, any act or service with respect to an ICTS Transaction, such as execution of any provision of a managed services contract or installation of software updates, is an ICTS Transaction on the date that the service or update is provided. Thus, if a person that is owned by, controlled by, or subject to the jurisdiction or direction of a

foreign adversary engages in an ICTS Transaction with a person subject to the jurisdiction of the United States on or after [Date of publication in the FEDERAL REGISTER], even if the service was provided pursuant to a contract initially entered into prior to [Date of publication in the FEDERAL REGISTER], that transaction is an ICTS Transaction that may be reviewed under this rule. The service is a new transaction separate from the underlying contract that will be subject to review by the Secretary.

§ 7.4 Determination of foreign adversaries.

As noted above, many commenters requested the Department identify those countries that it considers to be "foreign adversaries." Naming these countries, the commenters argued, would facilitate global trade by allowing U.S. businesses to assess the risks of certain types of ICTS Transactions from certain countries. It would also allow companies to adjust their supply chains to avoid the risks in such transactions, including the risk of an ICTS Transaction being reviewed, and possibly prohibited or modified, under this rule. Several commenters also noted that defining "foreign adversaries" would help determine, and possibly reduce, the adverse economic impact the rule may have on businesses through better business planning.

In response to these comments, the Department reconsidered its prior determination not to identify specific "foreign adversaries." The Department has determined that it is beneficial for the clarity of the rule, as well as for persons with ICTS Transactions that may be subject to the rule, to identify certain foreign governments and foreign non-government persons that are considered, solely for the purposes of the Executive Order, this rule, and any subsequent rules, to be "foreign adversaries." The list of foreign governments and foreign non-government persons this rule identifies as being "foreign adversaries" are: the People's Republic of China, including the Hong Kong Special Administrative Region (China); the Republic of Cuba (Cuba); the Islamic Republic of Iran (Iran); the Democratic People's Republic of Korea (North Korea); the Russian Federation (Russia); and Venezuelan politician Nicolás Maduro (Maduro Regime) . The

Secretary identified these foreign adversaries because they have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons, including taking actions and enacting policies that are inimical to the interests of the United States.

The determination to identify these "foreign adversaries" is based on multiple sources, including threat assessments and reports from the U.S. Intelligence Community, the U.S. Departments of Justice, State, and Homeland Security, and other relevant sources. Additionally, the Secretary will periodically review this list in consultation with appropriate agency heads and may add to, subtract from, supplement, or otherwise amend the list. Accordingly, this list may be revised at any time in the future. Any such changes will be announced in the Federal Register.

It is important to note that the list is solely for the purposes of the Executive Order, this rule, and any subsequent rules and does not reflect a determination by the United States about the nature of such foreign governments and foreign non-government persons for any purposes other than that ICTS Transactions with persons (as defined in this rule) owned by, controlled by, or subject to the jurisdiction or direction of an identified foreign adversary may pose an undue or unacceptable risk. Further, the rule states that 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.

§ 7.5 Effect on other laws.

Many commenters suggested that this rule should not apply if overlapping and existing U.S. authorities are in force, referencing in particular existing national security regulatory regimes. Specifically, commenters pointed to CFIUS; authorities under various National Defense Authorization Acts; the Export Administration Regulations; the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (*i.e.*, Team Telecom); and other programs under the authority of the Federal Communications Commission, the Department of Homeland Security, and the Office of the Director of National Intelligence.

Other commenters recommended exempting equipment provided by companies involved in mitigation agreements with the Federal Government.

This rule does not alter or affect any of these existing authorities; it is intended to complement, not supplant, these existing regimes. However, the Department understands the need for regulatory and business certainty, and in the interest of not duplicating efforts by other parts of the U.S. Federal government, the rule states that it does not apply to ICTS Transactions that CFIUS is actively reviewing, or has reviewed, as a covered transaction or covered real estate transaction or as part of such a transaction under section 721 of the Defense Production Act of 1950, as amended, and its implementing regulations. However, this exclusion in no way precludes a review of a subsequent ICTS Transaction if distinct from the previously CFIUS-reviewed transaction or new information is discovered.

Other provisions of the rule provide additional means of ensuring that any action taken by the Secretary neither conflicts with nor frustrates the purposes of other existing laws, regulations or processes. Thus, there are two separate points during the review process at which the Secretary is expressly required to consult with appropriate agency heads: before making an initial determination that the transactions is an ICTS Transaction that poses an undue or unacceptable risk (section 7.104) and before making a final determination (section 7.108). In requiring that the Secretary consult with other agency heads, the rule provides for a coordination mechanism with other agencies and Departments that have potentially overlapping jurisdiction. For example, before making an initial determination concerning a transaction, the review of which might potentially overlap with a review under CFIUS, the Secretary is required to consult with, among others, the Secretary of the Treasury, who serves as the Chairperson of CFIUS, thereby helping to ensure coordination and avoid redundancy.

In addition, section 7.100(a) of the rule provides that the Secretary may consider all relevant information provided by any U.S. Government national security body or other Federal Government agency, department or regulatory body in determining what action may be

necessary to ameliorate a threat posed by an ICTS Transaction.

Subpart B – Review of ICTS Transactions

Commenters largely recommended the final rule clarify the review process, requesting the specific criteria by which the Department will use to review transactions. As a whole, Subpart B adds a more detailed review process, as requested by commenters.

§ 7.100 – General.

§ 7.100(a) – Consideration of relevant information

Many commenters sought clarity as to the type of information on which the Secretary could base a determination to commence an evaluation of a transaction. In response to these comments, section 7.100(a) identifies sources or information, factors, and other variables related to a transaction that the Secretary may consider when reviewing a transaction. This list is non-exclusive and does not prevent the Secretary from reviewing any available information; the list is intended to provide parties to transactions with greater clarity about the types of materials on which the Secretary may rely when deciding whether to review (and during that review of) a transaction.

The rule states that the Secretary may consider information provided by any U.S. Government national security body or other Federal agencies. In addition, the rule clarifies that the Secretary, when making determinations about specific transactions, may also consider information that includes: (1) relevant public information; (2) confidential business or proprietary information; (3) classified national security information; (4) information from State, local, tribal, or foreign governments; (5) information from parties to a transaction, including records related to such transaction that any party keeps or uses, or would be expected to keep or use, in their ordinary course of business for such a transaction; (6) information obtained through the authority granted under sections 2(a) and (c) of the Executive Order and IEEPA; and (7)

information provided by any other U.S. Government agency, department, or other regulatory body.

The rule further revises section 7.100(a) to specify that information may be obtained through any administrative investigative or enforcement action undertaken pursuant to the authority granted under sections 2(a) and (c) of the Executive Order and IEEPA. The purpose of this clarification is to set out precisely the authorities that grant the Secretary the power to access and collect documents related to investigations and determinations of potentially prohibited transactions.

§ 7.100(c) – Determining Foreign Adversary involvement

In order to provide industry with more clarity regarding the determination of 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, the Department added guidance about what information it will consider when making these decisions. These factors include: (1) whether the party or its component suppliers have headquarters, research, development, manufacturing, test, distribution, or service facilities or other operations in a foreign country, including one controlled by a foreign adversary; (2) personal and professional ties between the party—including its officers, directors or similar officials, employees, consultants, or contractors—and any foreign adversary; (3) laws and regulations of the foreign adversary in which the party is headquartered or conducts operations, including research and development, manufacturing, packaging, and distribution; and (4) any other criteria that the Secretary deems appropriate.

§ 7.100(d) – Factors for determining an undue or unacceptable risk

Commenters also requested additional information from the Department about how it will determine whether an ICTS Transaction poses an undue or unacceptable risk. Along with listing

factors to help determine the relationship between a foreign party to an ICTS Transaction and a foreign adversary, the Department has provided guidance on some of the information that the Secretary, in consultation with the appropriate agency heads, will consider when determining the impact of an ICTS Transaction on U.S. national security.

Specifically, when determining whether an ICTS Transaction poses an undue or unacceptable risk, the Secretary and the appropriate agency heads will consider factors such as: (1) threat assessments and reports prepared by the Director of National Intelligence pursuant to section 5(a) of the Executive Order; (2) removal or exclusion orders issued by the Secretary of Homeland Security, the Secretary of Defense, or the Director of National Intelligence (or their designee) pursuant to recommendations of the Federal Acquisition Security Council, under 41 U.S.C. § 1323; (3) relevant provisions of the Defense Federal Acquisition Regulation and the Federal Acquisition Regulation, and their respective supplements; (4) entities, hardware, software, and services that present vulnerabilities in the United States as determined by the Secretary of Homeland Security pursuant to section 5(b) of the Executive Order, Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report," September 18, 2019; (5) actual and potential threats to execution of a "National Critical Function" identified by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency; (6) the nature, degree, and likelihood of consequence to the United States public and private sectors that could occur if ICTS vulnerabilities were to be exploited; and (7) any other source or information that the Secretary deems appropriate.

§ 7.100(d) - Risk Management

The Department specifically requested comments on transactions that could present an undue or unacceptable risk, but where that risk could be reliably and adequately mitigated or prevented. Commenters suggested creating national security risk categories for transactions and

providing assurance that the Secretary would impose the least intrusive measures to mitigate transactions in each category. Other commenters advocated creating risk categories or bands with different assessment approaches. The Department did not adopt these suggestions. ICTS Transaction reviews are made on a case-by-case basis. Therefore, categorically labeling transactions with pre-determined mitigation requirements would effectively counteract that individualized approach and may result in ICTS Transactions proceeding that otherwise should have been reviewed, and possibly prohibited or mitigated.

In determining whether an ICTS Transaction poses an undue or unacceptable risk, the rule clarifies the risk factors the Secretary, in consultation with the appropriate agency heads, may consider. Specifically, the Secretary may consider: (1) threat assessments and reports prepared by the Director of National Intelligence pursuant to section 5(a) of the Executive Order; (2) removal or exclusion orders issued by the Secretary of Homeland Security, the Secretary of Defense, or the Director of National Intelligence (or their designee) pursuant to recommendations of the Federal Acquisition Security Council, under 41 U.S.C. § 1323; (3) relevant provisions of the Defense Federal Acquisition Regulation and the Federal Acquisition Regulation, and their respective supplements; (4) entities, hardware, software, and services that present vulnerabilities in the United States as determined by the Secretary of Homeland Security pursuant to section 5(b) of the Executive Order, Department of Homeland Security Cybersecurity and Infrastructure Security Agency, “Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report," September 18, 2019; (5) actual and potential threats to execution of a “National Critical Function” identified by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency; (6) the nature, degree, and likelihood of consequence to the United States public and private sectors that could occur if ICTS vulnerabilities were to be exploited; and (7) any other source or information that the Secretary deems appropriate.

§ 7.101 Information to be furnished on demand.

The proposed rule contemplated that individuals might be requested to furnish the Secretary with information related to a transaction under review. Section 7.101 in this rule clarifies that, under the Secretary's authority pursuant to IEEPA, persons may be required to furnish under oath complete information relative to any ICTS Transaction under review. 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 may be required either before, during, or after an ICTS Transaction under review. Additionally, under the authorities provided by IEEPA, 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 electronic documents relating to any matter under investigation.

§ 7.102 - Confidentiality of information.

The proposed rule requested comments and recommendations from stakeholders on additional recordkeeping requirements for information related to transactions. Most commenters focused on the confidentiality and the public availability of any information received. Commenters strongly advocated that the Department protect confidential or proprietary business information when making or publishing reports. Some commenters advocated for more open publication of these reports, and how each threat was mitigated or eliminated.

To address these concerns and provide additional certainty for entities required to produce documents related to transactions, the rule clarifies the Department's responsibility to preserve the confidentiality of information requested by the Department. Specifically, the rule provides that information or documentary materials that are not otherwise publicly or

commercially available, submitted or filed with the Secretary under this part, will not be released publicly except to the extent required by law. However, the Secretary may disclose information or documentary materials, not otherwise publicly or commercially available: (1) pursuant to any administrative or judicial proceeding; (2) pursuant to an act of Congress; (3) pursuant to a request from any duly authorized committee or subcommittee of Congress; (4) pursuant to a request to any domestic governmental entity, or to any foreign governmental entity of a United States ally or partner, information or documentary materials, not otherwise publicly or commercially available and important to the national security analysis or actions of the Secretary, but only to the extent necessary for national security purposes, and subject to appropriate confidentiality and classification requirements; (5) where the parties or a party to a transaction have consented the information or documentary materials not otherwise publicly or commercially available may be disclosed to third parties; and (6) any other purpose authorized by law. These provisions largely incorporate the record release requirements of the Freedom of Information Act, 5 U.S.C. 552. While the Department will, as always, seek to protect business and other confidential information provided by parties, parties providing such information in response to this rule must clearly mark those documents as business or other confidential.

§ 7.103-Initial review of ICTS Transactions.

Many commenters addressed the manner in which an ICTS Transaction could be identified to the Secretary as a transaction that should be reviewed. In particular, many commenters sought clarity on the proposed provision that the Secretary could commence evaluations of transactions based on information received from private parties "that the Secretary determines to be credible." The commenters requested clear guidance on what types of information, or parties, the Secretary would deem credible. Additionally, several commenters noted that such a provision might incentivize parties to engage in anti-competitive behavior that would not necessarily lead to identifying transactions posing risks to national security. In light

of these comments and concerns, the rule clarifies that the Secretary may consider any referral for review of a transaction (referral): (1) upon receipt of any information identified in section 7.100(a); (2) upon written request of an appropriate agency head; or (3) at the Secretary's discretion. Following receipt of a referral, the Secretary will assess whether the referral falls within the scope of § 7.3(a) and involves ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction of direction of a foreign adversary, and determine whether to: (1) accept the referral and commence an initial review of the transaction; (2) request additional information, as identified in § 7.100(a), including information from the referring entity regarding the referral; or (3) reject the referral.

Several commenters requested the rule establish clearer procedures for how the Secretary will review ICTS Transactions. Commenters also advocated for differing determination timeframes, deadlines, or milestones based on device nature, threat severity, equipment replacement risks, and other potential harms.

In response to these and other comments, the Department provides that, unless the Secretary determines in writing that additional time is necessary, the Secretary shall issue the final determination within 180 days of accepting a referral and commencing the initial review of the ICTS Transaction. Regarding the procedures for the Secretary's review of ICTS Transactions, the Executive Order provides a careful process for the Secretary's decision-making. The rule further sets out the factors that the Secretary will consider to assist the decision-making process. Specifically, the rule provides that the Secretary shall assess whether the ICTS Transaction: falls within the scope of § 7.3(a) of the rule; 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. The Secretary will evaluate each transaction, on a case-by-case basis, based upon the particular facts and circumstances, including the identity of the parties involved.

The rule also further articulates what the Secretary will consider when determining

whether an ICTS Transactions poses an undue or unacceptable risk. The Department has identified ten criteria for such determinations. Along with other factors, when determining if an ICTS Transaction poses an undue or unacceptable risk, the Secretary will consider the nature of the information and communications technology or services at issue in the ICTS Transaction, including technical capabilities, applications, and market share considerations; the nature and degree of the direction or jurisdiction exercised by the foreign adversary over the design, development, manufacture, or supply at issue in the ICTS Transaction; and the statements and actions of the foreign adversary at issue in the ICTS Transaction. Other considerations include whether the ICTS Transaction poses a discrete or persistent threat and the nature of the vulnerability implicated by the ICTS Transaction.

§ 7.104 First interagency consultation.

The Department has clarified that the Secretary will consult with the appropriate agency heads after finding that an ICTS Transaction may fall within the scope of the Executive Order.

§ 7.105 Initial determination.

This rule clarifies that if, after review of an ICTS Transaction and consultation with the appropriate agency heads, the Secretary determines that such ICTS Transaction meets the criteria in section 7.103(c) of the rule, the Secretary shall then issue an initial written determination explaining the finding and whether the Secretary has determined to prohibit or propose mitigation measures to the ICTS Transaction at issue. The initial determination will contain no confidential information, even if such was relied upon to make the initial determination. Notice of this initial determination shall be served upon the parties to the ICTS Transaction known to the Secretary at the time of service. Service may be made by registered U.S. mail, facsimile, electronic transmission, or third-party commercial carrier, to an addressee's last known address or by personal delivery. Service of documents will be considered effective upon the date of

postmark, facsimile transmission, delivery to third party commercial carrier, electronic transmission or upon personal delivery. Notice of the initial determination to the parties may also be accomplished by publication in the Federal Register where the Secretary determines that the initial determination concerns or could impact entities beyond the parties to the ICTS Transaction, where one or more of the parties to the ICTS Transaction are unknown to the Secretary, or in any other circumstance at the Secretary's discretion.

§ 7.106 - Retention of records.

The proposed rule requested public comments on whether to require parties to undertake additional recordkeeping for information related to transactions. Some commenters argued that the Department should not impose additional recordkeeping requirements. Additionally, some commenters suggested that the recordkeeping requirement begin upon receipt of a transaction notice, rather than being an ongoing duty for any potentially prohibited ICTS Transaction.

After reviewing these comments, and consistent with IEEPA, the rule provides that, after receiving notification that an ICTS Transaction is under review or that an initial determination concerning an ICTS Transaction has been made, a notified person must immediately take steps to retain any and all records related to such transaction.

§ 7.107 – Procedures governing response and mitigation.

Commenters requested that the final rule explain how the Secretary's determinations may be "appealed" and how mitigation agreements will be reached and enforced. Commenters also sought more robust procedures for waivers, appeals, and mitigation. The proposed rule had provided that, within 30 days of a preliminary determination by the Secretary that a transaction was an ICTS Transaction that would pose an undue or unacceptable risk to the U.S. national security, parties to that transaction could submit a response to the decision. The proposed rule also allowed the Secretary to require a transaction be mitigated to reduce the risks the Secretary

identified in the preliminary determination.

In response to these comments, the Department has added provisions to enhance and clarify when and how parties to an ICTS Transaction that is the subject of an initial determination may engage with the Secretary about the initial determination. The rule establishes a clear process for responding to an initial determination concerning an ICTS Transaction and provides further guidance on how any identified risks may be mitigated so that an identified ICTS Transaction may proceed. Similar to the proposed rule, within 30 days of being notified of an initial determination, pursuant to section 7.105 of the rule, parties to that transaction may respond to the initial determination or assert that the circumstances leading to the initial determination no longer apply. A party may submit arguments or evidence in support of their response and may also propose remedial steps that the party believes would negate the basis for the Secretary's initial determination. The rule also allows parties to an ICTS Transaction that is subject to an initial determination to request a meeting with the Department, which may be granted at the Secretary's discretion. Additionally, the rule clarifies that if the parties to an ICTS Transaction do not submit a response to the Secretary's initial determination within 30 days following service of the initial determination, that initial determination will become final.

Other commenters recommended the adoption of an appeals process for parties notified of a final determination. The Department has adopted a process for reconsidering an initial determination by the Secretary. However, an administrative appeals process would hinder the Secretary's ability to move swiftly to prevent an undue or unacceptable risk.

Some commenters also requested that the Department establish a maximum life span for imposed mitigations, arguing that such a rule would reduce the inhibiting effects that mitigations would have on ICTS innovation. The Department disagrees with commenters, finding that such a clause would prevent the Department from evaluating the mitigations put in place on ICTS Transactions. Failing to reevaluate would effectively limit mitigation requirements and potentially reopen national security vulnerabilities.

§ 7.108 - Second interagency consultation.

The proposed rule set out the review process that must be followed before the Secretary issues a final determination that constitutes a final agency action. The process involved response periods, as well as possible extensions, given to any party affected by a preliminary determination. Commenters addressed communications regarding initial and final determinations within the context of this process. Some commenters suggested that the Secretary should collaborate with private industry when making determinations, similar to the process within the Department of Homeland Security's Supply Chain Risk Management Task Force. Similar comments were received advocating for the establishment of a mechanism for industry to seek guidance on specific work programs or participants involved.

The Department has declined to add specific provisions relating to collaborating with industry on ICTS Transaction determinations. However, in consideration of these comments there is now a provision explaining what factors and sources the Secretary will take into consideration during the second consultation. Specifically, the Secretary will take into account the views of the appropriate agency heads, through the interagency consultation processes. In providing their views, the appropriate agency heads may consider the perspective of relevant public-private working groups and advisory committees with which they convene or engage. For instance, DHS's views could incorporate input from the Supply Chain Risk Management Task Force. The Department also points out that it maintains a number of advisory committees that provide regular opportunities for industry and the regulated community to provide feedback to the Department on issues impacting their operations. Under the Secure and Trusted Communications Networks Act of 2020, the National Telecommunications and Information Administration is also charged with establishing a program to share supply chain risk information with telecommunication providers and manufacturers.

Commenters also requested that the Department explain whether and how the Secretary's

determinations may be appealed or reviewed by another authority. This rule adds a provision that, should any appropriate agency head oppose the Secretary's proposed final determination, the Secretary shall notify the President of the Secretary's proposed final determination and such opposition. After receiving direction from the President regarding the Secretary's proposed final determination and any appropriate agency head's opposition thereto, the Secretary shall issue a final determination pursuant to §7.109.

Additionally, the Department will implement, within 120 days of publishing this rule, procedures for how parties to a proposed, pending, or ongoing ICTS Transaction may seek a license, pursuant to Section 2(b) of the Executive Order, in a manner consistent with the national security of the United States.

As noted above, after reviewing an ICTS Transaction that the Secretary believes may pose an undue or unacceptable risk, the Secretary will engage in a first interagency consultation with the appropriate agency heads to discuss the ICTS Transaction and the Secretary's concerns. Following that consultation, the Secretary will make an initial determination and, if that decision includes a determination to prohibit an ICTS Transaction, will notify the parties to the transaction of the Secretary's initial determination. After the parties are afforded an opportunity to respond to the initial determination and propose mitigation measures, the Secretary will engage in a second interagency consultation with the appropriate agency heads, to discuss the transaction, the initial determination, and any response. This process will help ensure that all information regarding ICTS Transactions and the views of the appropriate agency head are considered when the Secretary makes a final determination.

§ 7.109 - Final determination.

As noted above, the Department appreciates the comments requesting additional clarity on the process by which the Secretary will make decisions about ICTS Transactions. The rule now provides a specific step for issuing final determinations on ICTS Transactions. The outcome

of a final determination remains unchanged from the proposed rule and will provide that an ICTS Transaction is either: (1) prohibited; (2) not prohibited; or (3) permitted pursuant to the adoption of agreed-upon mitigation measures. Moreover, the rule clarifies that the written final determinations will include directions on the timing and manner of cessation of a prohibited ICTS Transaction, as applicable, along with the penalties, as authorized by IEEPA, for violations of applicable mitigation terms or other direction or prohibition issued under this rule. The final determination will provide a specific description of the prohibited ICTS Transaction and shall be limited in force to the circumstances described therein. Moreover, if the Secretary determines that an ICTS Transaction is prohibited, the final determination shall direct the least restrictive means that the Secretary, in the Secretary's discretion, determines to be necessary to attenuate or alleviate the undue or unacceptable risk posed by the ICTS Transaction.

§ 7.109(c)– Notification of final determination

Commenters also provided a number of suggestions on how to further ensure the Secretary is held accountable for his or her actions under the authority of this rule. Recommendations include limiting the Secretary's ability to assign a designee with final decision-making authority and deleting the emergency action provision set forth in section 7.100(f) of the proposed rule. These suggestions are intended to ensure that Congress can hold the executive branch accountable for enforcement actions.

In response to these comments, the final rule enhances transparency by requiring final written determinations to be published in the Federal Register, where they are readily accessible to both the Congress and the public. Moreover, the rule now clarifies that the publication shall omit any confidential business information.

§ 7.200 - Penalties.

Commenters requested the final rule clarify the type and scope of penalties for

noncompliance with the Secretary's prohibition or mitigation of a transaction. We agree with commenters that the type and scope of the penalties for noncompliance were unclear, and the section has been revised accordingly. The rule now clarifies that any person who commits a violation of any final determination, direction, or mitigation agreement may be liable to the United States for civil or criminal penalties under IEEPA.

Other Comments:

The Department received other comments with which the Department disagrees. The Department responds to those comments below.

First, one commenter requested that the Department expand the meaning of the term "electronic means" within the definition of ICTS. While the Department cannot modify the definition of ICTS contained in the Executive Order, the Department clarifies that "electronic means" includes electromagnetic, magnetic, and photonic means. This change is not intended to widen the scope of the rule, but merely to clarify the means by which ICTS must function in order for the rule to apply.

Second, some commenters requested that the Department provide technical assistance for parties forced to alter ICTS infrastructure. However, the Department is unable to offer technical assistance at this time. Accordingly, the Department declines to implement any provision for technical assistance in the rule, and the parties to the transaction will bear the responsibility and cost of complying with any prohibition or mitigation measure.

Third, one commenter argued that the rule imposes an unfunded mandate on the private sector, within the meaning of the Unfunded Mandates Reform Act of 1995, Pub. L. 104-4 (UMRA), contrary to the determination made by the Department in the proposed rule. The commenter further argued that UMRA requires that before the rule becomes final, the Department must include in the rule a written statement assessing the costs and benefits of the rule, and estimates of future compliance costs, as required by UMRA. The Department continues

to believe that the rule does not constitute a "Federal private sector mandate" as defined by UMRA, in that the rule does not impose "an enforceable duty" upon the private sector. *See* 2 U.S.C. § 658(7). Rather, the rule sets out the processes and procedures that the Secretary of Commerce will use to identify, assess, and address certain transactions, including classes of transactions. However, as the commenter notes, when a rule does constitute a "Federal private sector mandate," UMRA requires the agency prepare a written statement containing information about the costs and benefits of the mandate, including, where feasible, future compliance costs, 2 U.S.C. § 1532, as well as that the agency identify and consider regulatory alternatives and select the least costly, most cost-effective, or least burdensome alternative that achieves the objectives of the rule, 2 U.S.C. § 1535. Thus, even in the event that the rule were considered to constitute a federal private sector mandate, the Department has met these requirements in full through the preparation of the accompanying Regulatory Impact Analysis.

Changes from the Proposed Rule:

Upon consideration of the public comments received, the Department makes several changes, as discussed in detail above, from the proposed rule in order to increase clarity and certainty for the public. First, the rule provides detail on the procedures the Secretary will follow when reviewing ICTS Transactions, including identifying the criteria and information the Secretary will consider. For example, the rule provides clarity as to when the Secretary will consult with the appropriate agency heads as part of the review and determination process. Second, the rule details the requirements for responding to initial determinations. Third, the rule clarifies that parties may respond to an initial determination or seek to negotiate a mitigation agreement with the Secretary. Fourth, the rule now provides that unless the Secretary determines in writing that additional time is necessary, the Secretary shall issue a final determination within 180 days of accepting a referral and commencing the initial review of an ICTS Transaction, eliminating the uncertainty of an open-ended review process. Fifth, the rule ensures

transparency by specifically requiring the Secretary to publish the results of final determinations, absent any confidential business information, in the Federal Register. Sixth, the rule now specifies that an ICTS Transactions between parties outside of a sector designated as critical infrastructure must involve a clearly specified technology or service in order to be considered a covered ICTS Transactions.

Additionally, in response to commenters seeking clarity regarding the scope of the rule, including numerous requests for the identification of "foreign adversaries," the Department defines certain terms. The added definitions help to clarify the scope of the rule by providing guidance on which entities may be subject to the rule, what constitutes an ICTS Transaction, and whether an ICTS Transaction involves a foreign adversary. This additional clarity will assist entities with making appropriate decisions regarding ICTS Transactions that may present risks to the national security, therefore helping to protect the United States' ICTS supply chain.

Classification

A. Executive Order 12866 (Regulatory Policies and Procedures)

Pursuant to the procedures established to implement Executive Order 12866, the Office of Management and Budget has determined that this rule is economically significant.

B. Executive Order 13771 (Reducing Regulation and Controlling Regulatory Costs)

This rule is not subject to the requirements of Executive Order 13771 because the benefit-cost analysis demonstrates that the regulation is anticipated to improve national security as its primary direct benefit.

ICTS has become integral to the daily operations and functionality of U.S. critical infrastructure, as well as much, if not most, of U.S. industry. Moreover, ICTS accounts for a large part of the U.S. economy. Accordingly, if vulnerabilities in the ICTS supply chain—composed of hardware, software, and managed services from third-party vendors, suppliers, service providers, and contractors—are exploited, the consequences can affect all users of that

technology or service, potentially causing serious harm to critical infrastructure, U.S. Government operations, and disrupting the United States and the global economy. These harms are already occurring. As noted in Executive Order 13873, "foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services, which store and communicate vast amounts of sensitive information, facilitate the digital economy, and support critical infrastructure and vital emergency services."

U.S. entities purchasing and incorporating ICTS equipment and using ICTS services, such as network management or data storage, provided by foreign adversaries can create multiple opportunities for foreign adversaries to exploit potential vulnerabilities in the ICTS. That, in turn, could cause direct and indirect harm to both the immediate targets of the adverse action and to the United States as a whole. Incorporation of a foreign adversary's software, equipment, and products into domestic ICTS networks, as well as the use of use of foreign cloud, network management, or other services, greatly increases the risk that potential vulnerabilities may be introduced, or that they may be present without being detected. These potential vulnerabilities are often categorized under the general concepts of threats to privacy, data integrity, and denial of service.

Some foreign actors are known to exploit the sale or lease of software and hardware to introduce vulnerabilities that can allow them to steal critical intellectual property, research results (e.g. health data), or government or financial information from users of the software or hardware. Such vulnerabilities can be introduced at the network, cloud service or individual product data, allow traffic monitoring or surveillance, and may be resistant to detection by private purchasers or telecommunications carriers. Once detected, the existence of such vulnerabilities may be extremely costly or impossible to remediate.

Vulnerabilities to data integrity can be created by including an adversary's hardware and software into U.S. networks and systems. This incorporated hardware and software could then pose opportunities to add or remove important information, modify files or data streams, slow

down, or otherwise modify the normal transmission or availability of data across U.S. networks. Such capabilities could be exercised in areas as diverse as financial market communications, satellite communications or control, or other sensitive consumer information. Privileged access to market movement and trends, or other manipulation, could disrupt and harm the operation of major exchanges.

A foreign adversary could also effectively deny access to critical services by exploiting vulnerabilities provided by the incorporation of hardware and software into U.S. environments, fully or partially shutting down critical networks or functions at key times. These types of attacks are known as denial of service attacks. Such attacks could cause widespread problems, such as if they occur during periods of crisis, or they could be used selectively by targeting individual corporations, infrastructure elements, or other important infrastructure functions. They could also be masked to make the source of the disruption difficult to attribute, and therefore be difficult to trace and terminate.

Such risks can be substantially increased by incorporating the software and equipment from unreliable adversaries into the U.S. telecommunications infrastructure. However, these risks are not necessarily confined to infrastructure environments. They could, for example, be present in the use of cloud services, as well as in the widespread use of some consumer devices, networked surveillance cameras, drones, or interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data.

The number of attacks by foreign adversaries on the ICTS supply chain are known to be increasing. The associated costs are borne by the U.S. Government as well as private industry. Given the ubiquity of ICTS in the modern economy and especially in critical infrastructure, the benefits of preventing significant disruptions or harms to the ICTS supply chain that could cause incalculable costs to U.S. firms, consumers, and the U.S. Government, would be very high.

This rule provides a process through which serious disruptions to the United States telecommunications infrastructure can be avoided or ameliorated. The rule provides the means of

bringing to bear the information and analytical resources of the U.S. government to address ICTS supply chain issues before they arise, and which may be beyond the means of individual telecommunications carriers or other U.S. ICTS purchasers or users to address on their own. As noted above, the costs associated with the potential attacks, loss of service, or disruption to the ICTS supply chain are not known at this time, and are in actuality unknowable due to the generally clandestine nature of the attacks and the fact that they may or may not occur. However, by deterring, preventing, or mitigating these attacks, this rule will provide the United States with substantial, though unknowable, economic benefits as well as benefits to the national security of the United States.

C. 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). 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) and has posted a final regulatory flexibility analysis (FRFA) as part of the RIA (*see* ADDRESSES). This final rule is likely to have a significant economic impact on a substantial number of small entities. A summary of the FRFA follows.

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 IRFA, a statement of the assessment of the agency of such issues, and a statement of any changes made in the proposed rule as a result of such comments.

Many commenters discussed the possibility that this rule could present significant economic costs. For example, one commenter stated that "Commerce's proposed rules would result in an extremely broad and unprecedented increase in regulatory jurisdiction over private ICT transactions. The notice of proposed rulemaking thus marks a watershed regulatory moment

for companies in or adjacent to the ICT market – which is to say, virtually every company in United States – given the government's newfound stance that it can determine key terms of what ICT companies can buy, sell, or use. As a result, this proceeding and the rules that result from it inescapably will impose additional costs on ICT companies, such as the increased practical need – even absent a legal requirement – to document supply chain risk management analysis in the event a transaction is investigated, along with related due diligence to consider the as-yet uncertain possibilities for government intervention." In the RIA, the Department estimated costs associated with developing and implementing a plan to conduct due diligence on potentially covered transactions, including estimating the number of small entities that could be affected by the rule and the economic impact on those small entities.

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, as well as in the preamble to the Notice of Proposed Rulemaking issued on November 27, 2019 (84 FR 65316), and are not repeated here.

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 the purpose of this analysis we define a small business as one employing fewer than 500 persons. This definition allows us to use 2017 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 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 less 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.

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 $235 million and $20.2 billion, or about $2,800 to $6,300 per entity. The Department estimated the costs to small entities using the same methodology. All small entity calculations and assumptions can be found in Tables 10 through 14. These tables are analogous to Tables 5 through 9 in the RIA. While most of the assumptions below are identical to those found in the previous estimates, there are 3 important adjustments to assumptions in the small entity cost estimates:

1. Entities potentially impacted by the rule reduced by 0.4 percent to account for our finding that 99.6 percent of all affected entities have less than 500 employees.
2. Small entities are less likely to have the resources to develop and implement a compliance plan. This analysis thus reduces estimates of the share of small firms likely to engage in these activities accordingly.
3. Small entities engage in fewer transactions than large entities. This analysis reduces the estimates of the number of transactions subject to the rule per small firm accordingly.

As a result of these adjustments, the Department estimates that costs to affected small entities will range between approximately $109 million and $10.9 billion, or about $1,800 and $3,900 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 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 rule. Small firms downstream of impacted industries are likely to face increases in the prices of ICT products they use as inputs and either absorb the increase in cost and/or raise their prices. Given this situation, it is possible that the rule will have a more substantial adverse impact on small firms relative to larger firms.

However, the changes made from the proposed rule benefit small businesses by limiting the scope of transactions subject to the rule. Small entities have fewer suppliers and engage in fewer transactions than large entities. As a result, by identifying specific foreign adversaries and providing guidance on which entities may be subject to the rule as well as additional criteria on what constitutes an ICTS Transaction, small entities will more readily be able to determine whether their transactions are subject to review under the rule – and may in some cases, find that none of their transaction are likely to be within the scope of the rule. Additionally, by specifically requiring the Secretary to publish the results of final determinations in the Federal Register, small businesses will be able to assess whether their transactions are substantially similar to those that have been prohibited. Finally, the rule reduces the potential burdens on small entities by emphasizing that (1) the Secretary will choose the least burdensome restriction

that still allows for protection of the national security when deciding whether to prohibit or mitigate an ICTS Transaction, and (2) the Secretary shall issue a final determination within 180 of commencing an initial review.

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 2017 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 less than 500 employees are $2.2 million. Thus, using our threshold of 500 employees we estimate that 99.6% of affected entities are small businesses which is likely a slight underestimate.

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 rule will allow the Secretary to review ICTS Transactions to determine whether they present an undue or unacceptable risk, a function which is currently not performed by any other private or public entity. As noted above, 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 the 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 two alternatives would achieve the goal of protecting the national security, nor would they eliminate the rule's significant economic impact on a substantial number of small entities.

First, the Department considered providing an exemption for small entities that have 5 or fewer employees. ("smallest entities"). According to Census Bureau's most recent dataset of number of firms by employee count, about 61% of all firms have less than 5 employees.

Second, the Department 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 items 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; and (c) ICTS Transactions under which a United States 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 either of these regulatory alternatives. Exempting certain industries or sectors or eliminating the application of the 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 rule's national security objectives. 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 as opposed to exempting entire industries, sectors, or regulated smallest entities from review.

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 agency shall explain the actions a small entity is required to take to comply with a rule or group of rules.

D. 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 rulemaking does not contain a collection of information requirement subject to review and approval by OMB under the PRA.

E. Unfunded Mandates Reform Act of 1995

This rule would not produce 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.

F. Executive Order 13132 (Federalism)

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

G. Executive Order 12630 (Governmental Actions and Interference with Constitutionally Protected Property Rights)

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

H. Executive Order 13175 (Consultation and Coordination with Indian Tribes)

The Department has analyzed this proposed 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.

I. 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.

List of Subjects in 15 CFR Part 7

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

This document of the Department of Commerce was signed on January 13, by Wilbur Ross, Secretary of Commerce. That document with the original signature and date is maintained by the Department of Commerce. For administrative purposes only, and in compliance with requirements of the Office of the Federal Register, the undersigned Department of Commerce Federal Register Liaison Officer has been authorized to sign and submit the document in electronic format for publication, as an official document of the Department of Commerce. This administrative process in no way alters the legal effect of this document upon publication in the Federal Register.

Signed in Washington, DC, on January 13, 2021.

Asha Mathew,

Federal Register Liaison Officer, U.S. Department of Commerce.

For the reasons set out in the preamble, 15 CFR part 7 is added to read as follows:

PART 7—SECURING THE INFORMATION AND COMMUNICATIONS TECHNOLOGY AND SERVICES SUPPLY CHAIN

Subpart A – GENERAL

Subpart B – REVIEW OF ICTS TRANSACTIONS

Authority: 50 U.S.C. 1701 *et seq.*; 50 U.S.C. 1601 *et seq.*; E.O. 13873, 84 FR 22689.

Subpart A—GENERAL

§ 7.1 Purpose.

These regulations set forth the procedures by which the Secretary may: (a) determine whether any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service (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; (b) issue a determination to prohibit an ICTS Transaction; (c) direct the timing and manner of the cessation of the ICTS Transaction; and (d) consider factors that may mitigate the risks posed by the ICTS Transaction. The Secretary will evaluate ICTS Transactions under this rule, which include classes of transactions, on a case-by-case basis. The Secretary, in consultation with appropriate agency heads specified in Executive Order 13873 and other relevant governmental bodies, as appropriate, shall make an initial determination as to whether to prohibit a given ICTS Transaction or propose mitigation measures, by which the ICTS Transaction may be permitted. Parties may submit information in response to the initial determination, including a response to the initial determination and any supporting materials and/or proposed measures to remediate or mitigate the risks identified in the initial determination as posed by the ICTS Transaction at issue. Upon consideration of the parties' submissions, the Secretary will issue a final determination prohibiting the transaction, not prohibiting the transaction, or permitting the transaction subject to the adoption of measures determined by the Secretary to sufficiently mitigate the risks associated with the ICTS Transaction. The Secretary

shall also engage in coordination and information sharing, as appropriate, with international partners on the application of these regulations.

§ 7.2 Definitions.

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

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

Department means the United States Department of Commerce.

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

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

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

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

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

Information and communications technology or services or ICTS means any hardware, software, or other product or service, including cloud-computing services, primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means (including electromagnetic, magnetic, and photonic), including through transmission, storage, or display.

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

Person means an individual or entity.

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

corporation, partnership, association, or other organization, wherever organized or doing business, that is owned or controlled by a foreign adversary.

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

Sensitive personal data means:

(1) Personally-identifiable information, including:

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

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

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

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

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

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

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

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

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

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

(2) Genetic information, which includes the results of an individual's genetic tests, including any related genetic sequencing data, whenever such results, in isolation or in combination with previously released or publicly available data, constitute identifiable data. Such results shall not include data derived from databases maintained by the U.S. Government and routinely provided to private parties for purposes of research. For purposes of this paragraph, "genetic test" shall have the meaning provided in 42 U.S.C. 300gg-91(d)(17).

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

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

§ 7.3 Scope of Covered ICTS Transactions.

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

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

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

(3) Is initiated, pending, or completed on or after [Insert Date of publication in the FEDERAL REGISTER], regardless of when any contract applicable to the transaction is entered into, dated, or signed or when any license, permit, or authorization applicable to such transaction was granted. Any act or service with respect to an ICTS Transaction, such as execution of any provision of a managed services contract, installation of software updates, or the conducting of repairs,

that occurs on or after [Insert Date of publication in the FEDERAL REGISTER] may be deemed an ICTS Transaction within the scope of this part, even if the contract was initially entered into, or the activity commenced, prior to [Insert Date of publication in the FEDERAL REGISTER]; and

(4) Involves one of the following ICTS:

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

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

(A) Wireless local area networks, including:

(*1*) Distributed antenna systems; and

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

(B) Mobile networks, including:

(*1*) eNodeB based stations;

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

(*3*) NodeB base stations;

(*4*) Home location register databases;

(*5*) Home subscriber servers;

(*6*) Mobile switching centers;

(*7*) Session border controllers; and

(*8*) Operation support systems;

(C) Satellite payloads, including:

(1) Satellite telecommunications systems;

(*2*) Satellite remote sensing systems; and

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

(D) Satellite operations and control, including:

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

(*2*) Satellite control centers;

(*3*) Satellite network operations;

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

(*5*) Satellite uplink centers;

(E) Cable access points, including:

(*1*) Core routers;

(*2*) Core networks; and

(*3*) Core switches;

(F) Wireline access points, including:

(*1*) Access infrastructure datalinks; and

(*2*) Access infrastructure digital loops;

(G) Core networking systems, including:

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

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

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

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

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

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

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

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

(*1*) Fiber optical cables; and

(*2*) Repeaters;

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

(A) Internet hosting services;

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

(C) Managed services; and

(D) Content delivery services;

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

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

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

(C) Drones or any other unmanned aerial system;

(v) Software designed primarily for connecting with and communicating via the Internet that is in use by greater than one million U.S. persons at any point over the twelve (12) months preceding an ICTS Transaction, including:

(A) Desktop applications;

(B) Mobile applications;

(C) Gaming applications; and

(D) Web-based applications; or

(vi) ICTS integral to:

(A) Artificial intelligence and machine learning;

(B) Quantum key distribution;

(C) Quantum computing;

(D) Drones;

(E) Autonomous systems; or

(F) Advanced Robotics.

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

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

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

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

§ 7.4 Determination of foreign adversaries.

(a) The Secretary has determined that the following foreign governments or foreign non-government persons have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons and, therefore, constitute foreign adversaries solely for the purposes of the Executive Order, this rule, and any subsequent rule:

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

(2) Republic of Cuba (Cuba);

(3) Islamic Republic of Iran (Iran);

(4) Democratic People's Republic of Korea (North Korea);

(5) Russian Federation (Russia); and

(6) Venezuelan politician Nicolás Maduro (Maduro Regime).

(b) The Secretary's determination of foreign adversaries is solely for the purposes of the Executive Order, this rule, and any subsequent rule promulgated pursuant to the Executive Order. Pursuant to the Secretary's discretion, the list of foreign adversaries will be revised as determined to be necessary. Such revisions will be effective immediately upon publication in the Federal Register without prior notice or opportunity for public comment.

(c) The Secretary's determination is based on multiple sources, including:

(1) National Security Strategy of the United States;

(2) The Director of National Intelligence's 2016-2019 Worldwide Threat Assessments of the U.S. Intelligence Community;

(3) The 2018 National Cyber Strategy of the United States of America; and

(4) Reports and assessments from the U.S. Intelligence Community, the U.S. Departments of Justice, State and Homeland Security, and other relevant sources.

(d) 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.

§ 7.5 Effect on other laws.

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

§ 7.6 Amendment, modification, or revocation.

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

§ 7.7 Public disclosure of records.

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

Subpart B---REVIEW OF ICTS TRANSACTIONS

§ 7.100 General.

In implementing this part, the Secretary of Commerce may:

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

(1) Publicly available information;

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

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

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

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

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

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

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

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

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

(1) Whether the person or its suppliers have headquarters, research, development, manufacturing, test, distribution, or service facilities, or other operations in a

foreign country, including one controlled by, or subject to the jurisdiction of, a foreign adversary;

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

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

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

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

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

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

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

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

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

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

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

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

§ 7.101 Information to be furnished on demand.

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

(b) For purposes of paragraph (a) of this section, the term “document” includes any written, recorded, or graphic matter or other means of preserving thought or expression (including in electronic format), and all tangible things stored in any medium from which information can be processed, transcribed, or obtained directly or indirectly, including

correspondence, memoranda, notes, messages, contemporaneous communications such as text and instant messages, letters, emails, spreadsheets, metadata, contracts, bulletins, diaries, chronological data, minutes, books, reports, examinations, charts, ledgers, books of account, invoices, air waybills, bills of lading, worksheets, receipts, printouts, papers, schedules, affidavits, presentations, transcripts, surveys, graphic representations of any kind, drawings, photographs, graphs, video or sound recordings, and motion pictures or other film.

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

§ 7.102 Confidentiality of information.

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

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

(1) Pursuant to any administrative or judicial proceeding;

(2) Pursuant to an act of Congress;

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

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

national security purposes, and subject to appropriate confidentiality and classification requirements;

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

(6) Any other purpose authorized by law.

(c) This section shall continue to apply with respect to information and documentary materials that are not otherwise publicly or commercially available and submitted to or obtained by the Secretary even after the Secretary issues a final determination pursuant to § 7.109 of this part.

(d) The provisions of 18 U.S.C. 1905, relating to fines and imprisonment and other penalties, shall apply with respect to the disclosure of information or documentary material provided to the Secretary under these regulations.

§ 7.103 Initial review of ICTS Transactions.

(a) Upon receipt of any information identified in § 7.100(a), upon written request of an appropriate agency head, or at the Secretary's discretion, the Secretary may consider any referral for review of a transaction (referral).

(b) In considering a referral pursuant to paragraph (a), the Secretary shall assess whether the referral falls within the scope of § 7.3(a) of this part and involves ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, and determine whether to:

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

(2) Request additional information, as identified in § 7.100(a), from the referring entity regarding the referral; or

(3) Reject the referral.

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

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

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

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

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

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

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

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

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

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

(i) Health, safety, and security;

(ii) Critical infrastructure;

(iii) Sensitive data;

(iv) The economy;

(v) Foreign policy;

(vi) The natural environment; and

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

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

(d) 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.

§ 7.104 First interagency consultation.

Upon finding that an ICTS Transaction likely meets the criteria set forth in § 7.103(c) during the initial review under § 7.103, the Secretary shall notify the appropriate agency heads and, in consultation with them, shall determine whether the ICTS Transaction meets the criteria set forth in § 7.103(c).

§ 7.105 Initial determination.

(a) If, after the consultation required by § 7.104, the Secretary determines that the ICTSTransaction does not meet the criteria set forth in § 7.103(c):

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

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

(b) If, after the consultation required by § 7.104, the Secretary determines that the ICTS Transaction meets the criteria set forth in § 7.103(c), the Secretary shall:

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

(i) Explains why the ICTS Transaction meets the criteria set forth in § 7.103(c); and

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

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

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

§ 7.106 Recordkeeping requirement.

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

§ 7.107 Procedures governing response and mitigation.

Within 30 days of service of the Secretary's notification pursuant to § 7.105, a party to an ICTS Transaction may respond to the Secretary's initial determination or assert that the circumstances resulting in the initial determination no longer apply, and thus seek to have the initial determination rescinded or mitigated pursuant to the following administrative procedures:

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

(b) A party may propose remedial steps on the party's part, such as corporate reorganization, disgorgement of control of the foreign adversary, engagement of a compliance monitor,

or similar steps, which the party believes would negate the basis for the initial determination;

(c) Any submission must be made in writing;

(d) A party responding to the Secretary's initial determination may request a meeting with the Department, and the Department may, at its discretion, agree or decline to conduct such meetings prior to making a final determination pursuant to § 7.109;

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

(f) If the Department receives no response from the parties within 30 days after service of the initial determination to the parties, the Secretary may determine to issue a final determination without the need to engage in the consultation process provided in section 7.108 of this rule.

§ 7.108 Second interagency consultation.

(a) Upon receipt of any submission by a party to an ICTS Transaction under § 7.107, the Secretary shall consider whether and how any information provided—including proposed mitigation measures—affects an initial determination of whether the ICTS Transaction meets the criteria set forth in § 7.103(c).

(b) After considering the effect of any submission by a party to an ICTS Transaction under § 7.107 consistent with paragraph (a), the Secretary shall consult with and seek the consensus of all appropriate agency heads prior to issuing a final determination as to whether the ICTS Transaction shall be prohibited, not prohibited, or permitted pursuant to the adoption of negotiated mitigation measures.

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

(d) After receiving direction from the President regarding the Secretary's proposed final determination and any appropriate agency head's opposition thereto, the Secretary shall issue a final determination pursuant to § 7.109.

§ 7.109 Final determination.

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

(1) Prohibited;

(2) Not prohibited; or

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

(b) Unless the Secretary determines in writing that additional time is necessary, the Secretary shall issue the final determination within 180 days of accepting a referral and commencing the initial review of the ICTS Transaction pursuant to § 7.103.

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

(d) The final determination shall:

(1) Be written, signed, and dated;

(2) Describe the Secretary's determination;

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

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

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

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

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

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

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

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

(2) The appropriate agency heads.

(f) The results of final written determinations to prohibit an ICTS Transaction shall be published in the Federal Register. The publication shall omit any confidential business information.

§ 7.110 Classified national security information.

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

Subpart C---ENFORCEMENT

§ 7.200 Penalties.

(a) Maximum penalties.

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

(2) *Criminal penalty*. A person who willfully commits, willfully attempts to commit, or willfully conspires to commit, or aids and abets in the commission of a violation of any final determination, direction, or mitigation agreement shall, upon conviction of a violation of IEEPA, be fined not more than $1,000,000, or if a natural person, may be imprisoned for not more than 20 years, or both.

(3) The Secretary may impose a civil penalty of not more than the maximum statutory penalty amount, which, when adjusted for inflation, is $307,922, or twice the amount of the transaction that is the basis of the violation, per violation on any person who violates any final determination, direction, or mitigation agreement issued pursuant to this part under IEEPA.

(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 notified party or parties.

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

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

(b) 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.

(c) 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.

[FR Doc. 2021-01234 Filed: 1/14/2021 4:15 pm; Publication Date: 1/19/2021]