This document is scheduled to be published in the Federal Register on 11/26/2021 and available online at **federalregister.gov/d/2021-25329**, and on **govinfo.gov**

DEPARTMENT OF COMMERCE

15 CFR Part 7

[Docket No. 211115-0230]

RIN 0605-AA62

Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications

AGENCY: U.S. Department of Commerce.

ACTION: Notice of Proposed Rulemaking.

SUMMARY: To implement provisions of Executive Order 14034, "Protecting Americans' Sensitive Data from Foreign Adversaries" (EO 14034), the Department of Commerce is proposing to amend its Interim Final Rule on Securing the Information and Communications Technology and Services Supply Chain (Supply Chain Rule), which was published on January 19, 2021, 86 FR 4909. Specifically, this proposed rule would amend the Supply Chain Rule to provide for additional criteria that the Secretary of Commerce (the Secretary) may consider specifically when determining whether ICTS Transactions (as defined in the Supply Chain Rule) that involve connected software applications present an undue or unacceptable risk. The rule also makes conforming changes by revising the definition of ICTS to expressly include "connected software applications" and adding a definition of "connected software application" that is consistent with that used in EO 14034. The Department is interested in the public's views on the additional criteria for connected software applications, including whether they should be applied to all ICTS Transaction reviews, whether there are other criteria that should be applied, and how the Secretary should apply the criteria to ICTS Transactions involving connected software applications.

DATES: Comments to this proposed rule must be received on or before [INSERT DATE 30 DAYS AFTER DATE OF 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-2021-0005.
- *By email directly to: ICTsupplychain@doc.gov.* Include "RIN 0605-AA62" 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, 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.*

FOR FURTHER INFORMATION CONTACT: Joseph Bartels, U.S. Department of Commerce, telephone: (202) 482-0224. For media inquiries: Brittany Caplin, Deputy Director of Public Affairs and Press Secretary, U.S. Department of Commerce, telephone: (202) 482-4883, email: PublicAffairs@doc.gov.

SUPPLEMENTARY INFORMATION:

Background

On January 19, 2021, the Department published an interim final rule in the Federal Register on "Securing the Information and Communications Technology and Services Supply

Chain." 86 FR 4909. The Supply Chain Rule implemented Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain" (84 FR 22689), including by setting out procedures by which the Secretary of Commerce, in consultation with the appropriate heads of other administrative agencies, would review ICTS Transactions for whether they present an undue or unacceptable risk due to a foreign adversary's involvement. The Supply Chain Rule defines "ICTS" as "any hardware, software, or other product or service, including cloud-computing services, primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means (including electromagnetic, magnetic, and photonic), including through transmission, storage, or display." The Supply Chain Rule further provides that an "ICTS Transaction" is, "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 EO 13873. The term ICTS Transaction includes a class of ICTS Transactions."

On June 9, 2021, the President issued EO 14034 to "elaborate upon measures to address the national emergency with respect to the information and communications technology and services supply chain that was declared in Executive Order 13873 of May 15, 2019, 'Securing the Information and Communications Technology and Services Supply Chain.'" EO 14034 sets out the finding "that the increased use in the United States of certain connected software applications designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary, which the Secretary of Commerce acting pursuant to EO 13873 has defined to include the People's Republic of China, among others, continues to threaten the national security, foreign policy, and economy of the United States." This rule would implement EO 14034 by specifically adding the term "connected

software applications" and the accompanying criteria, which do not appear in EO 13873, to the Supply Chain Rule to ensure the rule clearly and consistently identifies the ICTS that is threatened.

EO 14034 orders the Secretary to "evaluate on a continuing basis transactions involving connected software applications that may pose an undue risk of sabotage or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States; pose an undue risk of catastrophic effects on the security or resiliency of the critical infrastructure or digital economy of the United States; or otherwise pose an unacceptable risk to the national security of the United States or the security and safety of United States persons."

EO 14034 further sets out certain factors, consistent with the criteria established in EO 13873 and in addition to those set forth in the Supply Chain Rule, that should be considered in evaluating the risks of a transaction involving connected software applications. Specifically, EO 14034 lists the following as potential indicators of risk related to connected software applications: "ownership, control, or management by persons that support a foreign adversary's military, intelligence, or proliferation activities; use of the connected software application to conduct surveillance that enables espionage, including through a foreign adversary's access to sensitive or confidential government or business information, or sensitive personal data; ownership, control, or management of connected software applications by persons subject to coercion or cooption by a foreign adversary; ownership, control, or management of connected software applications by persons involved in malicious cyber activities; a lack of thorough and reliable third-party auditing of connected software applications; the scope and sensitivity of the data collected; the number and sensitivity of the users of the connected software application; and the extent to which identified risks have been or can be addressed by independently verifiable measures."

This proposed rule incorporates these potential indicators of risk as criteria to be considered by the Secretary when assessing whether an ICTS Transaction involving connected software applications poses an undue or unacceptable risk. The Department seeks public comments on these criteria, including how the Secretary should apply these to ICTS Transactions involving connected software applications, and whether there are additional criteria that should be considered by the Secretary with respect to connected software applications. The Department is also interested in the public's views as to whether these criteria should be applied to all ICTS Transaction reviews or just those that involve connected software applications. In addition, the Department seeks comment on any other considerations the Secretary should take into account when determining whether an ICTS Transaction involving connected software applications should, consistent with the authority and procedures of EO 13873 and the Supply Chain Rule, be allowed, mitigated, or prohibited.

Additionally, consistent with EO 14034's recognition of the ongoing threat, identified in EO 13873, by foreign adversaries to steal or otherwise obtain data through connected software applications, the Department notes that the term "information and communications technology and services" encompasses "connected software applications" and is proposing to revise the definition of ICTS accordingly to expressly so specify. This rule would also make a conforming revision to the term "ICTS Transaction," and would define "connected software applications" as "software, a software program, or a group of software programs, that is designed to be used on an end-point computing device and includes as an integral functionality, the ability to collect, process, or transmit data via the internet."

Section 7.1 Scope

The Department proposes to add the phrase "connected software applications" to section 7.1 of Title 15 of the Code of Federal Regulations (CFR).

Section 7.2 Definitions

As noted above, consistent with EO 14034's recognition of the ongoing threat by foreign adversaries to steal, otherwise obtain, or disrupt data through connected software applications, this rule would expressly specify that the term "information and communications technology and services or ICTS" encompasses "connected software applications." The proposed definition of "connected software applications" is taken from EO 14034: "software, a software program, or a group of software programs, that is designed to be used on an end-point computing device and includes as an integral functionality, the ability to collect, process, or transmit data via the internet."

The Department welcomes comment on whether this definition is sufficient to identify fully this category of ICTS, or whether further clarification or elaboration is needed. For instance, are there technical aspects to the definition that are used in industry or engineering that should be incorporated into the definition? Should the Department include other devices, such as those that communicate through short message service (SMS) messages, or low-power radio protocols? Should the definition be extended from "end-point" devices to "end-to-end" technology, and is "end-to-end" a term of art that we should employ? Are there other means of communication or transmission that are not encompassed by this definition but should be included?

Section 7.3 Scope of covered transactions

Further, the Department proposes to add new § 7.3(a)(4)(v)(E) regarding the types of software "designed primarily for connecting with and communicating via the Internet that is used by greater than one million U.S. persons" involved in ICTS Transactions that are subject to the Secretary's review.

Section 7.103 Initial review of ICTS Transactions

To incorporate the new criteria for determining whether a transaction involving connected software applications poses an undue or unacceptable risk, as defined in the Supply

Chain Rule, this rule would amend § 7.103 to add the criteria from EO 14034 in a new paragraph. Notably, these criteria complement, and are in addition to, the criteria already in 7.103(c) for determining whether an ICTS Transaction poses an undue or unacceptable risk. In making this determination for connected software applications, the Secretary would evaluate both the criteria in 7.103(c) and in the new paragraph. Specifically, the Department would redesignate current paragraph 7.103(d) as 7.103(e) and add new paragraph 7.103(d) to include the following criteria:

- ownership, control, or management by persons that support a foreign adversary's military, intelligence, or proliferation activities;
- use of the connected software application to conduct surveillance that enables espionage, including through a foreign adversary's access to sensitive or confidential government or business information, or sensitive personal data;
- ownership, control, or management of connected software applications by persons subject to coercion or cooption by a foreign adversary;
- ownership, control, or management of connected software applications by persons involved in malicious cyber activities;
- a lack of thorough and reliable third-party auditing of connected software applications;
- the scope and sensitivity of the data collected;
- the number and sensitivity of the users of the connected software application; and
- the extent to which identified risks have been or can be addressed by independently verifiable measures.

As noted above, while the proposed regulatory text below adds these criteria in a new sub-paragraph applicable only to ICTS Transactions involving connected software applications, the Department is also inviting comments on whether these criteria are sufficient or whether others should be added. For example, should the Department add a criterion such as whether the software has any embedded out-going network calls or web server references, regardless of the ownership, control, or management of the software?? The Department also seeks comments on whether the criteria should be more generally applicable to ICTS Transactions.

With regard to the phrase "ownership, control or management," should it be understood to include both continuous control/management and sporadic control/management (e.g., when a third-party must be temporally granted access to apply updates/upgrades/patches/etc.), or should this phrase be further clarified?

Additionally, the Department seeks comment on whether and how the Department should specifically define the terms "reliable third-party" and "independently verifiable measures," and, if so, whether there are generally accepted definitions or terms of art that the Department should consider adopting. The Department is also interested in whether the reference to "third-party auditing of connected software applications" is sufficiently clear or whether it needs further definition. For example, would it be understood to apply to audits by a third party of only the connected software applications, or to audits of the organizations implementing the software applications as well? Also, should the requirement to audit applications be revised to make clear that auditing is a continuous process through the development and deployment life cycle of the application? And would the requirement to audit applications be understood to refer only to source-code examination and verification, or would it also include monitoring of logs or other data that the application collects?

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 significant but not economically significant.

C. **Regulatory Flexibility Analysis**

The Chief Counsel for Regulation of the Department of Commerce certifies to the Chief Counsel for Advocacy of the Small Business Administration that this proposed rule would not have a significant economic impact on a substantial number of small entities. The factual determination for this determination is as follows.

This proposed rule would update the regulations at 15 CFR Part 7 that implement EO 13873 to revise the term ICTS to specifically include "connected software applications," as well as to affirm that a transaction involving connected software applications is an ICTS Transaction. It would add criteria the Secretary and the appropriate agency heads may use in making determinations about the risks potentially posed by ICTS Transactions involving connected software applications. The rule would also make conforming changes.

Accordingly, this proposed rule does not increase the scope of applicability of the existing regulations, the economic effects of which were evaluated in the regulatory impact analysis (RIA) associated with the Supply Chain Rule, at 86 FR 4909. (The RIA can be found online at reginfo.gov, and at regulations.gov, with a search for RIN 0605-AA51.) This proposed rule, once implemented, will not add any costs or burdens to any entity, small or large, because it does not expand the application scope of the Supply Chain Rule. Because this proposed rule neither increases the number of entities to which the Supply Chain Rule applies, nor increases the cost and burdens on those entities, it would not have a significant economic impact on a substantial number of small businesses.

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

F. Executive Order 13132 (Federalism)

This proposed 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 proposed 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.

Dated: November 16, 2021

_____

Trisha Anderson
Deputy Assistant Secretary for Intelligence and Security
U.S. Department of Commerce

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

1. The authority citation for part 7 continues to read as follows:

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

2. Revise § 7.1 to read as follows:

Subpart A—GENERAL

§ 7.1 Purpose.

(a) These regulations set forth the procedures by which the Secretary may:

(1) Determine whether any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service (ICTS Transaction), including connected software applications, 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;

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

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

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

(b) The Secretary will evaluate ICTS Transactions under this rule, which include 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.

3. Amend § 7.2 by adding, in alphabetical order, the definition for "Connected software application" and revising the definition of "Information and communications technology or services or ICTS" to read as follows:

§ 7.2 Definitions.

* * * * *

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

* * * * *

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

* * * * *

4. Amend § 7.3 by adding paragraph (a)(4)(v)(E) to read as follows:

§ 7.3 Scope of Covered ICTS Transactions.

(a) * * *

(4) * * *

(v) * * *

(E) Connected software applications; or

* * * * *

5. In § 7.103, redesignate paragraph (d) as paragraph (e) and add new paragraph (d) to read as follows:

§ 7.103 Initial review of ICTS Transactions.

* * * * *

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

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

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

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

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

(5) A lack of thorough and reliable third-party auditing of connected software applications;

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

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

(8) The extent to which identified risks have been or can be addressed by independently verifiable measures.

* * * * *

[FR Doc. 2021-25329 Filed: 11/24/2021 8:45 am; Publication Date: 11/26/2021]