U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

January 11, 2022

Ms. Trisha Anderson
Deputy Assistant Secretary for Intelligence and Security
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

Re: Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications; Docket No. DOC-2021-0005; RIN: 0605-AA62

Dear Ms. Anderson:

The U.S. Chamber of Commerce (Chamber) submits the following comments in response to the U.S. Department of Commerce's (Department) notice of proposed rulemaking to amend its interim final rule (IFR) on Securing the Information and Communications Technology and Services (ICTS) Supply Chain to integrate the additional criteria provided under Executive Order 14034 (EO), "Protecting Americans' Sensitive Data from Foreign Adversaries."[1]

At the outset, it is important to remind the Department that the underlying IFR continues to be extremely problematic. The overly broad nature of the IFR and the absence of any clarity regarding the types of transactions of interest to the administration is exceptionally challenging for the business community. However, this rulemaking recognizes the legitimate security concern that foreign adversaries may look to exploit connected software applications for purposes contrary to the national security interests of the United States. Some of the additional criteria provided under the EO are valuable to help guide investigations by the Secretary of Commerce in determining if certain transactions involving connected software applications present an undue or unacceptable risk. We have several comments below intended to refine the rulemaking before it is finalized.

The Administration Should Develop More Clear Guidelines and Risk Mitigation Strategies

Any discussion of bolstering the federal government's tools to stop problematic connected software application transactions must include a recognition of the need for a federal comprehensive ICTS supply chain strategy, including the need to protect the information and communications technology and services provided and used in the United States. ICTS are indispensable in today's business environment. U.S. businesses of all sizes are integrating ICTS applications into nearly all aspects of their operations, and this trend will accelerate as companies

[1] Executive Order 14034, "Protecting Americans' Sensitive Data from Foreign Adversaries," (86 Fed. Register 31423, June 9, 2021)

continue to embrace mobile and cloud computing. While ICTS are responsible for helping realize enormous economic growth, they are increasingly the targets of foreign adversaries.

Yet, mitigating against these attacks is a moving target and mounting challenge. Supply chains are increasingly complex global networks comprised of large and growing volumes of third-party partners who need access to data and assurances they can control who sees that data. Today, new stress and constraints on staff and budget, and rapid changes to strategy, partners, and the supply and demand mix, add further challenges and urgency. At the same time, more knowledgeable and security conscious customers and employees are demanding transparency and visibility into the products and services they buy or support.

This presents significant challenges to the U.S. business community, but the reality is the federal government's approach is of limited value in helping to stop foreign adversary attacks. ICTS is among some of the most powerful and complex technologies in use today. The race to develop and improve their capabilities is intensive and global in scale. Supply chain risks include geopolitical risks that could sever a supply chain, as well as risks stemming from inconsistent standards and development practices. This rule's approach to pursue case-by-case investigations, based on broadly defined criteria, and impose control measures is insufficient to securing the ICTS supply chain. Further, it casts a cloud of uncertainty over myriad U.S. business transactions involving ICTS. The Department's transaction review scheme creates regulatory uncertainty for a large segment of the U.S. economy and threatens to overwhelm the Department's resources by the sheer volume of ICTS transactions potentially in scope. As a regulatory tool, transaction reviews will be neither scalable nor effective in this context.

Therefore, the Department should develop as part of a comprehensive strategy performance-based guidelines and risk mitigation strategies to help U.S. businesses identify and avoid problematic connected software transactions. We recommend the Department utilize a process incorporating the business community's perspective in developing these guidelines, similar to the National Institute of Standards and Technology work in developing the *Cybersecurity Framework.*[2] Doing so would provide an additional tool to U.S. businesses while leveraging the administration's efforts to protect the security, integrity, and reliability of ICTS technologies beyond a small number of investigations. The Department could further encourage the business community to adopt these guidelines and strategies voluntarily by declaring that transactions governed by these guidelines would not fall under review. This approach would provide needed tools to help the U.S. business community mitigate the risks of transactions involving connected software while avoiding an unpredictable regulatory burden.

"Connected Software Applications" Definition Demonstrates Dynamic ICTS Environment

The addition of "connected software transactions" is an important delineation of the broader ICTS definition, but arguably "connected software transactions" are already covered under the IFR. For example, below are several instances where the definition of "connected software transactions" closely aligns with other covered activities under the IFR (with areas of comparison in *italics and underlined*):

[2] National Institute of Standards and Technology, *Cybersecurity Framework.* https://www.nist.gov/cyberframework

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. (Definition from Rulemaking)

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.* (from: § 7.2 Definitions)

~~~~~~~

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;
(from: § 7.3(a)(4)(iii))

This overlap in definitions underscores the dynamic operating environment of many ICTS transactions and exemplifies that the overall IFR suffers from being overly broad. It also complicates the U.S. business community's efforts to identify problematic ICTS transactions while navigating a potentially uncertain regulatory environment where the Department may apply multiple standards in reviewing ICTS transactions. If the Department maintains this specific definition in the final rule, we recommend that it provide more specific guidance as discussed above and propose specific mitigation measures to help the U.S. business community identify and address ICTS supply chain risks.

The Potential Risk Indicators Should Be Applied to All ICTS Transactions Under Review

The overlap in definitions covering "connected software applications" could potentially establish inconsistent reviews for ICTS transactions – depending on whether or not the Department determines a potentially problematic transaction as a "connected software application" transaction or something similar – with the proposed risk indicators being applied in one instance and not the other. We would propose instead that the new risk indicators be applied to *all* ICTS transactions and not just those deemed "connected software applications." This
~~~~~~~

would provide consistent review criteria for all transactions that fall under the IFR rule, providing greater certainty and consistency to the U.S. business community in understanding what factors will be considered in any potential investigation.

Conclusion

Thank you for the opportunity to comment on the Department's proposal. Our members support efforts to secure ICTS transactions against foreign adversaries and other malicious actors. We appreciate the Department's efforts to improve the current IFR. We look forward to continuing to work with the Department and other federal agencies to help solve the critical challenges in securing the ICTS supply chain.

Sincerely,

Christopher D. Roberti
Senior Vice President
Cyber, Intelligence,
and Supply Chain Security Policy

John Drake
Vice President
Supply Chain Policy