ITI Promoting Innovation Worldwide

January 11, 2022

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

RE: ITI Comments Responding to Commerce Department NPRM on Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications (RIN 0605-AA62; DOC-2021-0005)

Dear Deputy Assistant Secretary Anderson:

The Information Technology Industry Council (ITI) appreciates the opportunity to continue engaging with the Department of Commerce ("Commerce") as it seeks to implement Executive Order 14034, *Protecting Americans' Sensitive Data From Foreign Adversaries* via the Interim Final Rule that implements Executive Order 13873, *Securing the Information and Communications Technology and Services Supply Chain*.

The Information Technology Industry Council (ITI) is the premier global advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, manufacturing and related industries.

Most of ITI's members service the global market via complex supply chains in which technology is developed, made, and assembled in multiple countries, and service customers across all levels of government and the full range of global industry sectors, such as financial services, healthcare, and energy. We thus acutely understand the importance of securing global ICT supply chains as not only a global business imperative for companies and customers alike, but as critical to our collective security. As a result, our industries have devoted significant resources, including expertise, initiative, and investment in cybersecurity, to include data security, and supply chain risk management efforts to create a more secure and resilient Internet ecosystem.

Of paramount importance to ITI and its member companies is our shared commitment to addressing risks to global information and communications technology (ICT) supply chains and we recognize that data security plays an important role in protecting Americans from harm. We believe it is imperative that government and industry work together to achieve

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

the trusted, secure, and reliable global ICT supply chain that is essential for protecting national security and an indispensable foundation for supporting innovation and economic growth.

We have engaged with the Commerce Department throughout the development and implementation of the procedures associated with EO 13873. Based on our continued engagement, we offer some general comments on the NPRM at the outset, followed by responses to some of the specific questions that are posed in the NPRM.

General Comments

In general, we appreciate that the proposed rule attempts to maintain consistency in the review of connected software transactions by utilizing the established process under the ICTS Supply Chain IFR, and that it ties the Executive Order 13873 and Executive Order 14034 together, streamlining the regulations and the transaction review process. Indeed, streamlining supply chain regulation has been a perennial ITI recommendation to the USG.[1] We also appreciate that Commerce has continued to seek industry input as it develops measures to implement these two Executive Orders and encourage consistent future engagement with industry to ensure that resulting regulations are effective, efficient, and workable.

At the same time, we believe the NPRM unfortunately suffers from many of the same problems as the Interim Final Rule which it aims to amend. ITI continues to have substantive and procedural concerns with the Commerce Department's proposals. We fear that both the NPRM and Interim Final Rule as currently formulated introduce regulatory uncertainty into the globalized software marketplace in which American companies are key industry participants. We remain concerned that the IFR and now the NPRM's breadth coupled with the broad discretion granted to the Secretary of Commerce will continue to cast a cloud of uncertainty over almost all ICTS transactions and could undermine the national security objectives they purport to address, while also severely hindering U.S. competitiveness and hurting U.S. businesses.

Before addressing the specific questions posed in the NPRM we believe it is worth reiterating these concerns.

The highest risk ICTS transactions are not clearly identified. The definition of ICTS transactions remains so broad as to encompass nearly any economic activity within the technology or software services industries. While we appreciate the need to evaluate national security risks, such an all-encompassing scope threatens to overwhelm the

[1] See for example, recommendations that we proposed in ITI Federal Supply Chain White Paper and ITI Supply Chain Security Policy Recommendations, available here: https://www.itic.org/documents/public-sector/ITI_SupplyChain_Whitepaper_033021.pdf and https://www.itic.org/policy/ITI_SupplyChain_Principles2021.pdf

Department's resources. Setting aside potential due process concerns, this leaves industry without any realistic possibility of forecasting government action to undertake preventative mitigations.

Commerce seems to be taking a somewhat backwards approach in that the NPRM delineates a specific evaluation process and criteria for one specific class of ICTS transactions, while simultaneously leaving the IFR itself broad, implicating a limitless array of other ICTS transactions. While some may interpret this NPRM as suggestive that Commerce may be most interested in "connected software applications" and related transactions as the ICTS transactions most likely to be reviewed by Commerce, given that five subpoenas were issued pursuant to the overarching IFR and it remains intact the NPRM has in fact added to the confusion. Commerce needs to be more explicit in providing clarity on its approach to reviewing ICTS transactions.

As we recommended in our response to the IFR, Commerce and the USG needs to determine a way to identify specific categories of transactions that pose the highest potential national security risk and communicate those categories to industry. While we understand the general concern around foreign adversaries' accessing sensitive data, not every connected software application poses a risk, much in the same way that every ICTS transaction involving foreign adversaries does not pose a risk. In order to facilitate appropriate enforcement and compliance, the USG must articulate why certain transactions are problematic, instead of leaving it to industry to guess as to what national security risk the USG is trying to address.

Upon doing this, and assuming the pre-clearance/licensing process is still slated to be carried out consistent with the March 29 Advance Notice of Proposed Rulemaking, Commerce could meaningfully prioritize a review of such identified high-risk transactions in the voluntary pre-clearance/licensing process and provide industry with the necessary guidance to help internally identify high-risk transactions.

Reviews should be scoped to a limited set of ICTS providers. Commerce should also clearly define a class of entities to which the ICTS transaction review process will apply. Although the IFR articulates specific foreign adversaries, the definition of a "person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" is exceedingly broad. In fact, it arguably covers most American multi-national corporations that conduct business globally in jurisdictions identified as "foreign adversaries." In particular, this definition covers any entity that "acts . . . at the order, request, or under the direction or control of a foreign adversary." Orders or requests are undefined, but it is conceivable that court orders, subpoenas, or civil discovery could fall within these categories. Correspondingly, mere compliance with court orders in foreign jurisdictions could potentially subject American companies to the Interim Final Rule—certainly an incongruous policy outcome. Leaving this uncertainty in place will result in significant chilling of beneficial economic activity with no articulable reduction of national security risk. Commerce should therefore clearly articulate a standard or criteria regarding this

definition, similar to standards set by other transaction review regimes such as the Committee on Foreign Investment in the United States.

The national security risks posed by ICTS transactions are not clearly articulated. Rules governing the review of ICTS transactions by the Department of Commerce must be informed by a clear statement of the national security risks which such reviews are intended to remediate. Without clearly articulated policy goals, industry cannot effectively comment on the Department's proposals and therefore any final rules will likely be significantly overbroad and ineffective. It is our view that the NPRM does not clearly communicate the risks posed by connected software applications. This problem is not unique to this NPRM but is in fact an issue with the broader IFR as well.

The federal government has significant experience in reviewing private-sector transactions. Invariably, the most effective reviews have a clear policy goal and articulable triggers for scrutiny. For example, Hart-Scott-Rodino (HSR) Act reviews by the Department of Justice and the Federal Trade Commission (FTC) are largely successful at preventing consumer harm and protecting competition. Industry welcomes the predictability that clear purpose and jurisdictional thresholds bring to commercial activity. The Department of Commerce should duplicate the experience and existing processes of its sister agencies and clearly define risks that will be considered in connection with ICTS transaction reviews so that industry participants are on notice of the parameters.

The rulemaking process has been haphazard and remains incomplete. We submitted comments in April responding to the ANPRM issued by the Commerce Department on the pre-clearance/licensing process associated with the Interim Final Rule. This process was supposed to be implemented by May 19, 2021. However, to date, there has not been any formal update or implementation of a voluntary pre-clearance process. We once again stress the importance of having such a process in place in order to provide industry with the certainty it needs to continue to do business internationally. This process is also relevant to this NPRM, as parties that want to enter into a transaction that may implicate "connected software applications" would also benefit from a licensing program that would provide additional certainty as to whether the transaction would be subject to review.

ITI and other members of industry also submitted comments on the Interim Final Rule earlier this year, recommending a series of changes that we believed would strengthen the rulemaking by narrowing the scope and reducing ambiguity for industry, among other things. It was our understanding that the rule would be revised to reflect public comments. However, as with the proposed pre-clearance/licensing process, there have not been any updates to the IFR. To reemphasize points we made in our March 2021 submission, there are several areas of the IFR that need to be significantly clarified and/or reconsidered in order to make the rule workable, including related to the scope and breadth of the rule.

For example, we highlighted that the IFR was, at the time of publication, too broad to be practically implementable, going well beyond what is necessary to protect national security

and address undue security risks to critical infrastructure supply chains. Given the fact that Commerce has yet to publish a substantive revision of the IFR, we must reiterate our still valid concern that the IFR remains overbroad and riddled with implementation challenges. As a result, the IFR continues to cast a cloud of uncertainty over nearly all ICTS transactions with any nexus to the United States, including those that present no or low risks to national security. Barring changes, we continue to believe the rule will hinder innovation and undermine U.S. competitiveness. Until Commerce addresses previously submitted industry comments, the introduction of this NPRM, which adds "connected software applications" as an explicit class of ICTS technology, only serves to engender more uncertainty in the business community.

Further, we have overarching questions around the need for this specific set of implementing measures, when it seems clear that the original broadly scoped ICTS EO and IFR captures all transactions related to connected software; what such an approach means for other classes of ICTS transactions; and whether this approach is scalable or sustainable. For example, does Commerce anticipate similarly laying out different sets of criteria for other specific classes of ICTS technology, and will those sets of criteria be divergent from, and/or also considered in addition to, the broad criteria already laid out in part 7.103 of the IFR? If there are no plans to call out other classes of ICTS technologies in a similar manner, Commerce should issue guidance that makes this clear.

Questions Posed in the NPRM

General questions

1) *Should additional criteria be considered by the Secretary with respect to connected software applications?*

As referenced at the outset, this approach raises questions for industry as to how it may impact other classes of ICTS technology. Indeed, the fact that Commerce has delineated and proposed evaluation criteria only for connected software applications raises the question of whether different evaluation criteria will be established for different classes of ICTS technology or whether connected software applications are the primary focus of ICTS reviews generally. We do not advocate that Commerce pursue such a dual-track or indeed multiple-track approach involving both broad overarching review criteria, and slightly more specific criteria pertaining to a series of identified specific classes of ICTS.

The IFR itself already includes a list of evaluation criteria that the Secretary may rely upon in undertaking a review of a particular ICTS transaction in §7.103. It would seem that the already very broad criteria listed in §7.103 already seeks to evaluate and/or capture the risks associated with connected software applications and in some cases, subsumes the more specific evaluation criteria that is proposed in the NPRM.

For instance, the IFR proposes evaluation based on the severity of the harm posed by the ICTS Transaction on any one of several factors, which includes sensitive data.[2] It seems repetitive, then, to also delineate a separate but more specific set of criteria around "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" as it would seem espionage could be constituted as harm, and therefore already incorporated in the criteria laid out in the IFR. In addition to this, we encourage Commerce and the Secretary to consider, as an additional evaluation criterion, whether a derogation in the availability, confidentiality, or integrity of connected software applications would impact an important national interest. We also recommended this as an additional criterion in our response to the IFR. Indeed, the vast majority of products and services, to include connected software applications, would not affect a national interest and would thus not constitute an undue or unacceptable risk.

However, we believe that the approach that would provide the greatest clarity and business certainty would be for Commerce to identify the specific universe of classes of ICTS transactions that engender national security concerns, similar to how it has done with respect to connected software, rely upon specific and narrow review criteria and mechanisms to evaluate whether national security risks are triggered by specific transactions involving those classes of ICTS, and eliminate entirely the broad and ambiguous scope of the IFR which implicates all ICTS as subject to review. In the case of this NPRM, we suggest relying upon the newly introduced criteria *over* the criteria listed in the IFR as it is more specific and therefore lends itself to a more targeted approach.

2) *Should these criteria be applied to all ICTS Transaction reviews or just those that involve connected software applications?*

As mentioned in our response to the prior question, Commerce should consider how to maintain consistency between the two sets of evaluation criteria, and also consider the significant impact this NPRM will have on other classes of ICTS technology as Commerce introduces a new set of criteria specifically for connected software applications.

Keeping this in mind, we offer some additional perspectives on the evaluation criteria. We believe that some of the criteria that the NPRM proposes adding to the IFR is sensible. For example, the criteria around ownership, control or management by persons that support an adversary's military, intelligence, or proliferation activities, or whether the connected software is used to conduct espionage seem to be reasonable evaluation criteria and thus, could make sense to apply to a broader set of ICTS transactions.

However, as we mentioned above, some of this criterion is duplicative of the IFR (see for example, §7.103 of the IFR, which also lists "(2) The nature and degree of the ownership, control, direction, or jurisdiction exercised by the foreign adversary over the design,

[2] See 15 C.F.R. § 7.103

development, manufacture, or supply at issue in the ICTS Transaction" as evaluation criteria). Therefore, adding this language specifically for the evaluation of connected software transactions could result in redundancies and confusion. That being said, the language of this specific set of criteria in the NPRM seems more focused than the criteria set forth in the IFR. As such, we recommend including the NPRM evaluation criteria language over the existing IFR language.

Some of the criteria introduced in the NPRM raises additional questions. For instance, it is not clear to us how the number of users of a connected software application necessarily translates to a national security risk. Commerce should specifically articulate this. We also have questions about what is meant by "independently verifiable third-party measures" as well as questions around the "reliable third-party auditing" criteria and believe Commerce should work with industry to define these terms more clearly. We explore these concerns further and offer additional considerations in response to questions 8-10 below.

3) *Are there 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 E.O. 13873 and the Supply Chain Rule, be allowed, mitigated, or prohibited?*

The Secretary should also consider exempting from review an ICTS transaction that involves connected software if such software adheres to globally recognized international standards. As we referenced in our original response to the ICTS Supply Chain NPRM, we recommend that Commerce explore how and in what circumstances a company's adherence to certain risk-management standards or principles could be considered as mitigating factors. Standards to consider as mitigating include those laid out in the NIST Cybersecurity Framework, the ISO/IEC 27000 series, and standards compiled by the ICT Supply Chain Risk Management Task Force.[3] It is also worth noting that NIST is undertaking work to develop guidelines on software supply chain security, which could be leveraged here as well.

Definitions

Connected software applications*: 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.*

As a general matter, we believe that the definition of "connected software applications" is so broad as to be almost meaningless. Indeed, almost all software applications integrate

[3] See Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report (September 2019).

the functionality to collect, process, or transmit data in some way. Similar to our prior comments on the definition of ICTS in the IFR, this definition needs to be narrowed in order to be useful. We encourage Commerce to contemplate whether it can make this definition more specific. One way to do so would be to narrow the scope based on the *type* of data the software application is processing – i.e., sensitive data, vs. non-personal data, etc.

4) *Are there technical aspects to the definition that are used in industry or engineering that should be incorporated into the definition?*

At present, it is not clear in what parts of the software distribution and usage chain the NPRM will apply. We suggest that Commerce clarify whether the connected software applications rules contemplated in the NPRM will apply to some or all stakeholders across the software distribution and usage chain, including operators of the mobile operating system on which applications are installed, operators of distribution platforms for the downloading and installation of applications, and users who download and install the applications on their devices. To the extent certain rules are intended to apply to some of these stakeholders and not others, Commerce should make that clear. There are practical and policy implications associated with how Commerce approaches this. We recommend Commerce recognize that security of any sort is a shared responsibility and add information to the NPRM or definition accordingly. This will lend additional clarity to the rulemaking. As an example, the security of software applications running in the cloud should be the application owner's responsibility, whereas the cloud service provider is responsible for protecting the infrastructure on which such applications run.

5) *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?*

The definition should not be extended from "end-point" to "end-to-end." End-to-end is not a particularly useful concept when talking about connected services. Especially if the service being provided is cloud-based, there is an entire technology stack that is incorporated into the XaaS offering. End-to-End implies a simple client/server networking arrangement that does not account for the complexities of cloud environments.

6) *Are there other means of communication or transmission that are not encompassed by this definition but should be included?*

In the *Background* section of the NPRM, Commerce notes that the term "information and communications technology and services" encompasses "connected software applications." All of the other devices, technology, etc. outlined in the definition above are thus also encompassed by the broader ICTS definition. Commerce's net approach seems to be *both* to keep the ICTS definition broad, while at the same time identifying very specific types of ICTS that may create national security risk.

The ramifications of this dual track approach manifest in what amounts to a double review regime, as indicated later in the NPRM: "In making this determination for connected software applications, the Secretary would evaluate both the criteria in 7.103(c) and in the new paragraph (which lays out the evaluation criteria specific to connected software applications.) Such an approach seems both inefficient, burdensome, and not scalable.

Criteria

7) *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?*

We believe that the definition of "connected software application" as drafted already sufficiently covers such criteria (see, in particular, the term "transmit"), so adding this as an additional criterion would be redundant. However, we again highlight the need to further narrow this definition in order to make it useful.

8) *Should the criteria be more generally applicable to ICTS Transactions?*

We offer thoughts on this in response to question 2 above. In every instance where possible, Commerce should rely upon more specific criteria, such as that set forth in the NPRM, over the broad criteria listed in the IFR. Please refer to that section for more detail.

9) *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?*

One of the challenges in utilizing this as a criterion for evaluation of connected software applications is that "ownership, control, and management" constantly shifts. The premise of the question seems to recognize this as it asks whether this specific criterion should be understood to mean continuous control/management *and* sporadic control. Because software is continuously updated and patched, it would be unfeasible to conduct an evaluation every time a third-party is granted access to apply updates/patches, and also not scalable. Commerce should further narrow this phrase to "ownership" by referring to the Office of Foreign Asset Control's 50 Percent Rule to determine whether an entity is an owner. The rule states that "[blocked] persons…are considered to have an interest in all property and interests in property of an entity of which such blocked persons own,

whether individually or in the aggregate, directly or indirectly, 50 percent or greater interest."[4]

Once again, we think it useful to point out, however, that "the nature and degree of ownership, control, direction, or jurisdiction exercised by a foreign adversary over the design, development, manufacture, or supply at issue in the ICTS transaction" is already listed as evaluation criteria in the IFR itself.[5] That said, it seems this would introduce duplicative criteria for the Secretary to consider. It would therefore be useful to streamline the criteria and make them as specific as possible.

Finally, there are other USG initiatives currently being undertaken to address software supply chain security. For example, Section 4 of President Biden's *Executive Order on Improving the Nation's Cybersecurity,* is focused explicitly on "enhancing software supply chain security" and directs NIST to develop guidance to help improve software supply chain security. We highlight NIST's recently developed Secure Software Development Framework (SP 800-317), which provides a security framework for developers to apply in the software development life cycle, and which addresses issues around ownership, control, and maintenance to some extent. We encourage the Department to leverage this work and incorporate it into the IFR. For example, under the proposed voluntary licensing process, there could be a general license for ICTS transactions involving technology that meets these standards.

10) *Should the Department specifically define the terms "reliable third-party" and "independently verifiable measures," and, if so, are there generally accepted definitions or terms of art that the Department should consider adopting?*

Yes, we believe Commerce should further specifically define these terms. At present, it is not clear who/what constitutes a reliable third-party, nor do we understand what is meant by "independently verifiable measures." In seeking to further define these terms, Commerce should leverage international standards, including SOC 2 and ISO/IEC 27007, which both provide guidelines for conducting audits. Beyond that, Commerce should ensure that any ensuing guidelines are developed in conjunction with industry and take into account risk mitigation measures that industry may be deploying.

11) *Is the reference to "third-party auditing of connected software applications" sufficiently clear or does it need 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*

[4] See OFAC's Guidance on 50 Percent Rule here: https://home.treasury.gov/system/files/126/licensing_guidance.pdf
[5] See 15 C.F.R. § 7.103

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?

We believe the reference to "third-party auditing of connected software applications" requires additional definition. As we mentioned earlier in our submission, we have concerns about this being incorporated into the IFR for a number of reasons. First, interpreting this phrase to mean "source-code examination and verification" as well as "monitoring of logs and other data" is troubling, as such examination could implicate business/trade secrets and compromise sensitive IP. We have, on every occasion, pushed back against the examination of source code as a means to promote security and/or as a condition to do business in countries around the world, most notably China. If the USG were to interpret this phrase to mean government review of source code, we are concerned about the precedent it would set for countries globally. Indeed, it may spur countries to similarly require source-code reviews and log monitoring.

Second, without addressing the question of where within the software distribution and usage supply chain this NPRM applies, it is difficult to understand what is meant by an "third-party auditor." Commerce should clarify where this NPRM applies, and upon doing so, further make clear that a third-party auditor means a Registrar or Certification Body.

Third, this criterion seems to introduce an auditing process, which has not yet been well-established. Relying upon this criterion, then, seems premature at best. It is not clear whether this would be a new auditing process or whether it would leverage prior processes already in place. We discourage Commerce from introducing a new auditing requirement for software and instead suggest that it relies upon existing audits and/or certifications as a means to demonstrate that a particular application meets this criterion. If Commerce decides to further define this term as it moves forward, we encourage the agency to collaborate with industry to understand current auditing standards and frameworks used by the private sector, and how those might apply in this instance.

***

We appreciate the opportunity to provide our input into the rulemaking process. In developing a rule to implement EO 14034, we further appreciate that Commerce is seeking to leverage existing processes established under the Interim Final Rule so as not to unnecessarily complicate an already complex supply chain landscape by creating separate, unaligned review regimes. In doing so, however, Commerce must further consider how the two rules interrelate and more narrowly define terms introduced in the NPRM.

We encourage Commerce to continue to seek industry feedback as it moves forward with this NPRM, as well as the IFR more broadly, to ensure that resulting regulations provide a narrowly tailored, clear, scalable process that will provide certainty to business, strengthen

our collective security, and allow for continued U.S. technological leadership and competitiveness. Please consider ITI a resource moving forward. We are always happy to share further thoughts.

Sincerely,

John S. Miller
Senior Vice President of Policy
and General Counsel

Courtney Lang
Senior Director of Policy