March 22, 2021

U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

Via email to: ICTsupplychain@doc.gov

RE: Securing the Information and Communications Technology and Services Supply Chain – Interim Final Rule [RIN 0605-AA51]

BSA | The Software Alliance appreciates the opportunity to comment on the Department of Commerce's ("Department's") interim final rule implementing provisions of Executive Order 13873 "Securing the Information and Communications Technology and Services Supply Chain."[1]

As global leaders in development of quality, secure and trustworthy software, BSA's members share the Department's goal of enhancing the security and resiliency of the information and communications technology and services ("ICTS") supply chain.[2] The ICTS ecosystem fundamentally requires effective risk management to function and stakeholders across the value chain must work together to build trust in this environment on which they mutually rely. With these goals in mind, BSA recently published a white paper for "Building a More Effective Strategy for ICT Supply Chain Security," explaining why the U.S. must shift emphasis to an assurance-based approach, coordinated across government agencies with a strategic focus.[3]

BSA appreciates the Department's effort to clarify certain key terms and outline a formal interagency process for transaction review. However, even with revisions in the IFR, BSA remains concerned that the scope and nature of the proposed rules will at best marginally

---

[1] 84 Fed. Reg. 4909-4928 (Jan. 19, 2021) ("IFR" or "rules"); Executive Order 13873, *Securing the Information and Communications Technology and Services Supply Chain*, 84 Fed. Reg. 22689 (May 15, 2019) ("E.O. 13873").

[2] BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, CNC/Mastercam, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[3] BSA Position Paper, "US: Building a More Effective Strategy for ICT Supply Chain Security," (Feb. 16, 2021), https://www.bsa.org/policy-filings/us-building-a-more-effective-strategy-for-ict-supply-chain-security.

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

improve supply chain security, while severely constraining the ability of U.S. companies to innovate – undermining the technological leadership of U.S. industry and the global leadership of the U.S. government in developing sound, forward-looking technology policy.[4] The breadth of the authorities contemplated by the IFR combined with the vague criteria by which they can be invoked and the opaque processes for evaluating transactions will ultimately undermine industry's ability to create compliance programs with a predictable and reliable understanding of the risks. Because many of these concerns arise from the Executive Order that gave rise to this proceeding, we urge the Commerce Department to consider suspending the effective date of the IFR to allow for a more thorough evaluation of the Order's approach to supply chain security. However, should the Commerce Department elect to proceed, we offer the following specific recommendations to the Department in refining its rules as one among a set of tools to enhance the security of the ICTS ecosystem.

The Department Should Establish the Voluntary Licensing Regime Before Acting Under the Rules.

The Executive Order underlying the IFR expressly contemplated that a voluntary licensing system for pre-approval of transactions would be part and parcel of the review framework (see Section 2(b), referencing "procedures to license transactions otherwise prohibited pursuant to this order"). The IFR bifurcated the development of these rules, by putting the licensing regime on a separate track such that those procedures are not being published until March 22 and will not be implemented until May 19, 2021. Most importantly, these procedures should make clear in explicit terms that the default setting for private commercial ICTS transactions is that companies do not need to seek pre-approval; that, instead, as with customs rulings, this new ICTS transaction review regime establishes a narrow set of circumstances in which companies' due diligence with regard to ICTS transactions might trigger the need to seek U.S. government licensing and pre-approval based on a reasonable standard of care.

To this end, the Department should:

(1) Propose voluntary licensing procedures that clarify the narrow circumstances in which it may be prudent for parties to ICTS transactions to seek pre-approval;
(2) Seek comment on these proposed licensing procedures before implementing them; and
(3) Defer or eliminate the current May 19 deadline to ensure that any licensing regime can be developed in tandem with the other rules rather than on a separate, expedited track.

If anything, the licensing regime should be put in place substantially earlier than the broader review framework, to allow companies an opportunity to seek relief in connection with certain transactions that could possibly draw scrutiny before any such scrutiny begins. In addition, this pre-approval should be deemed "rulings" or "pre-guidance" to clarify the function of this process to industry participants and other stakeholders. Without a material understanding of how this process will work and an ability to become pre-cleared, companies will not be able to create responsive compliance regimes and transactions across the ICTS market will be stalled amid uncertainty.

---

[4] BSA Comments on Securing the Information and Communications Technology and Services Supply Chain, (Jan. 10, 2021), https://www.regulations.gov/document/DOC-2019-0005-0011 ("BSA NPRM Comments").

The Department Should Tailor These Rules Narrowly to the Problem They Are Designed to Address While Recognizing that Other Solutions May More Effectively Manage ICTS Supply Chains Overall.

Recognizing the diverse and widespread nature of entities with an interest in protecting U.S. networks, government efforts to address the serious threats facing ICTS supply chains have been prevalent in recent years, but have lacked strategic focus, often conflating national security and economic objectives.[5] Although the government may need to act swiftly to bar specific suppliers of concern from sensitive networks in some cases, policies that incentivize positive behavior will more effectively raise the level of security across the ICTS ecosystem in the long term. Assurance policies create incentives for companies to adopt best practices and improve the technology used to protect the supply chain, focusing on risk management that is more nuanced and tailored to the current environment, and more agile to adapt to future threats, than interventionist approaches.[6]

As the Department refines its IFR process, it should ensure the Department exercises this authority only where necessary to address an identified threat and where concrete and articulable security benefits will outweigh the political, economic, and other costs of this extraordinary intervention in the commercial ICTS market. Action under the IFR as written would not have, for example, prevented the recently revealed compromise of SolarWinds, wherein the adversary inserted malware through the software build process of a domestic supplier as a vector to disguise itself as normal traffic.[7] In this case, experts point to improvements such as industry standards for secure software design, better incident reporting and information sharing, and IT modernization to increase the cost of malicious activity and enhance collaborative response capabilities going forward.[8]

The Department Should Design These Rules as Part of a Holistic Framework that May Inform the Approach of Like-Minded Nations.

Due to the complex and global nature of ICTS supply chains, U.S. companies rely on transactions with companies based in a range of foreign countries to remain competitive. Any government review of commercial transactions, particularly one with potential retroactive application, must be narrowly tailored, transparent, and rooted in good governance principles

---

[5] *See* BSA White Paper at 1.

[6] *Id.* at 5-6.

[7] Kevin Mandia, "Prepared Statement of Kevin Mandia, CEO of FireEye, Inc. before the United States Senate Select Committee on Intelligence" at 1-3 (Feb. 23, 2021), https://www.intelligence.senate.gov/sites/default/files/documents/os-kmandia-022321.pdf ("Mandia Testimony").

[8] *See e.g.* Mandia Testimony at 3-5; Sudhakar Ramakrishna, "Written Testimony of Sudhakar Ramakrishna, Chief Executive Office, SolarWinds, Inc." at 4-5 (Feb. 23, 2021), https://www.intelligence.senate.gov/sites/default/files/documents/os-sramakrishna-022321.pdf; Brad Smith, "Strengthening the Nation's Cybersecurity: Lessons and Steps Forward Following the Attack on SolarWinds" at 10-15 (Feb. 23, 2021), https://www.intelligence.senate.gov/sites/default/files/documents/os-bsmith-022321.pdf; George Kurtz, "Testimony on Cybersecurity and Supply Chain Threats" at 3-7 (Feb. 23, 2021), https://www.intelligence.senate.gov/sites/default/files/documents/os-gkurtz-022321.pdf.

such that the U.S. would welcome the emulation of this process by allies and other like-minded governments – rather than invite protectionist retaliation.

For decades, the United States has leveraged the power of multilateral policy action, and the corresponding impact on global markets, in scenarios ranging from financial sanctions against bad actors to (more recently) promoting trusted suppliers in 5G communications infrastructure by virtue of the Prague Proposals.[9] The U.S. government should follow this model here. In practice, given the complexity of global ICTS markets and the potential for widespread disruption and economic damage from indiscriminate application of these U.S. transaction review authorities, this means that the U.S. government should conduct these reviews only in extremely rare circumstances in which the threat to U.S. interests is concrete, articulable and recognizable to U.S. allies and like-minded governments.

With this in mind, BSA offers the following concrete recommendations to tailor the IFR to meet the Department's goals:

- **Scope the Department's review, by:**
    - *Adopting a criticality assessment methodology.* The Department should adopt a methodology, perhaps drawing on the criticality assessment developed by the Department of Homeland Security's ("DHS") Cybersecurity and Infrastructure Security Agency ("CISA") in response to E.O. 13873, to tie its transaction reviews to the nexus between articulable foreign adversary threats, specific criticality assessments, and related risk management considerations.[10]
    - *Targeting companies controlled by a foreign adversary.* The Department should limit the scope of its review to transactions in which a foreign adversary has a controlling interest. This would appropriately focus the Department's review to circumstances in which a foreign [entity/adversary] would have the kind of leverage necessary to exploit a company's participation in the ICTS supply chain.[11]
    - *Modifying the following definitions*:
        - "Dealing in" should be defined – consistent with the definition of "dealer" in Section 3(a)(5) of the Securities Exchange Act of 1934 –

[9] *See* Government of the Czech Republic, "Prague 5G Security Conference announced series of recommendations: The Prague Proposals" (Mar. 5, 2019), https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

[10] *See* CISA, "Executive Order 13873 Response: Methodology for Assessing the Most Critical Information and Communications Technologies and Services" (Apr. 2020), https://www.cisa.gov/sites/default/files/publications/eo-response-methodology-for-assessing-ict_v2_508.pdf.

[11] BSA NPRM Comments at 7.

as "engaging directly in a financial transaction for the offering, buying, selling, or trading of prohibited ICTS."[12]

- "Use" should be defined as "employing ICTS for its intended purpose," to ensure that it excludes circumstances where ICTS is used outside the scope of its permitted use.[13]

- "ICTS Transaction" should be clarified to include only inbound transactions and exclude information in the public domain, cost updates, and repairs.[14] Consistent with the nature of the national security emergency declared in E.O. 13873, the Department should amend Section 7.3 of the IFR to clarify that the rules apply only to transactions in which the ICTS in question enters the United States or is provided and used in the United States by U.S. persons. [15] Furthermore, the Department should clarify that the definition of "ICTS transaction" explicitly excludes information in the public domain, as well as information regarding no cost updates and repairs. Currently, the IFR does not specify whether the ICTS transaction includes use of information in the public domain without the exchange of payment between the parties. U.S. companies generally do not track transactions of this nature and the rule should not inadvertently require U.S. companies to allocate the substantial resources that would be needed to police such transactions. Likewise, non-commercial transactions (e.g., transactions made for charitable or donative purposes) may necessarily involve costs incurred by the donor that are not recoverable. Due to the relative level of investment required, the definition's potential application to free or no cost transactions involving information in the public domain could have an outsized stifling effect on these types of critical transactions. In addition, subjecting free or no cost updates or repairs that are necessary for the security of ICTS on commercial transactions or uses that are not necessarily in the public domain to a review process countermands the underlying national security objectives.

- *Excluding low risk and non-domestic transactions.* Specifically, the Department should exclude from review transactions:

  - Where the ICTS products in question: (1) "connect to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements" – to ensure parties to those transactions are not forced to disconnect critical services operating in foreign countries; and (2) "cannot route or redirect user data traffic or permit visibility

---

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] E.O. 13873 (stating that to address the threat of ICTS emanating from foreign adversaries, "additional steps are required to protect the security, integrity, and reliability of information and communications technology and services *provided and used in the United States*" (emphasis added).

into any user data or packets that such equipment transmits or otherwise handles" – to avoid wasting the Department's resources on transactions posing little to no risk to national security.[16] By adopting these exceptions, the Department would align the rules with exceptions already recognized by Congress in the context of suppliers posing a national security threat to the ICTS supply chain.

  - That: (i) are intracompany transactions, including wholly owned foreign subsidiaries; (ii) involve technologies that meet objective benchmarks for supply chain security, such as International Standards Organization ("ISO") standards and forthcoming guidance from the DHS ICT Supply Chain Risk Management Task Force; or (iii) have gone through CFIUS review (as the IFR now provides) and/or other comparable review processes (such as those in the customs and export contexts).[17] Reviewing transactions that meet any of these three criteria would be duplicative and unnecessary.

- **Specify what constitutes a "foreign adversary."** The Department should define "foreign adversaries" more narrowly to capture specific providers or specific elements of the governments in question – for instance, specific Russian, Chinese, and Iranian intelligence services or related organizations – that the U.S. government believes are foreign adversary threats in the context of ICTS transactions. The Department should also clarify what constitutes "undue risk" so that companies can take appropriate steps to avoid such risk proactively.

- **Eliminate private party submissions.** Although the IFR expands on the process by which the Secretary will analyze private-party referrals—nominally requiring the Secretary to weigh the referral against the procedures established in the rules—in practice, the IFR grants the Secretary broad discretion to determine whether to act on such referrals and does not provide a threshold for what type of information may be submitted.[18] Moreover, the IFR does not establish a process by which a party subject to review would receive, at the very least, a summary of the information provided by a private party if that information triggered review. Although companies may be subject to obligations to submit accurate information to the Department under existing statutes such as the False Statements Act, without a response from the company with the product at issue, it may be difficult for the Department to assess the accuracy and completeness of the information it has received or to understand if that information is false or misleading. Given the pathway this provision paves for anticompetitive behavior, the Department should eliminate such private party submissions in the IFR process.[19] At minimum, the Department should include a process for entities to review and respond to any private party information provided to Commerce that prompts review of a transaction.

---

[16] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L 115-232 (Aug. 13, 2018), Sec. 889(a)(2), (b)(3), 132 Stat. 1917, codified at 41 U.S.C. § 3901.

[17] BSA NPRM Comments at 7-8.

[18] *See* IFR at § 7.103(b).

[19] *See* BSA NPRM Comments at 5-6.

- **Incorporate procedural safeguards.** The Department should incorporate some of BSA's previous recommendations to provide necessary procedural protections, specifically by:
    - Adopting Congressional oversight mechanisms that would include annual reports to committees of jurisdiction; and
    - Ensuring that the transaction review process is overseen by an Under Secretary-level designee with political accountability.[20]

* * * * *

BSA appreciates the opportunity to provide input on this IFR and looks forward to working with the Department as it engages with interagency partners in a holistic effort to enhance the security of the U.S. ICTS supply chain.

Sincerely,

Christian Troncoso
Senior Director, Policy

[20] *Id.* at 8-9.