January 10, 2020

Henry Young
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 [RIN 0605-AA51]

Dear Mr. Young:

BSA | The Software Alliance welcomes this opportunity to comment on the rules proposed by the Department of Commerce (Department) to govern the process and procedures for the review of transactions under the May 15, 2019 Executive Order ("Securing the Information and Communications Technology and Services Supply Chain").[1] BSA is the leading trade association representing the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, developing cutting-edge solutions in use across the information and communications technology (ICT) sector, and are global leaders in advancing best practices for developing quality, secure, and trustworthy software.[2]

BSA's members share the Department's interest in securing the ICT supply chain. To that end, BSA developed the "BSA Principles for Good Governance: Supply Chain Risk Management" to guide effective policy responses and assist industry and government in evaluating national supply chain risk management policies.[3] These principles feature an

---

[1] 84 Fed. Reg. 65316 (Nov. 27, 2019) ("NPRM").

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

[3] *BSA Principles for Good Governance: Supply Chain Risk Management*, https://www.bsa.org/files/policy-filings/07172019bsasupplychainprinciples.pdf.

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

emphasis on risk management, interoperability, transparency, discretion, enforcement, collaboration, fairness, and research and development. Consideration of such consensus principles is of critical importance here, where the Department is not merely refining an existing regulatory model but creating one from the ground up, with short-term and long-term implications for the entire ICT industry and for how the US government approaches security challenges going forward.

We have significant concerns that, when measured against these principles, the NPRM does not set forth a workable framework for securing the ICT supply chain. Under this proposal, the Secretary of Commerce (Secretary) would have unbounded discretion to review commercial ICT transactions, applying highly subjective criteria in an ad hoc and opaque process that lacks meaningful safeguards for companies. Collectively and individually, the present proposal's defects would leave industry in an inescapable quandary. It would be impossible for companies to create responsive compliance programs or to conduct business with a predictable and reliable understanding of the risks. As a result, the NPRM's proposed framework would likely have only a marginal impact on improving supply chain security, while severely constraining US companies' ability to innovate – undermining both the technological leadership of US industry and the global leadership of the US government in developing sound, forward-looking technology policy.

The broad scope of the NPRM, coupled with its vaguely defined standards, will put US companies at a competitive disadvantage. The ICT supply chain is complex and global; no one country owns all the pieces in the value chain. Therefore, investment in foreign countries helps US companies maintain their leadership. Uncertainty about whether any particular transaction could be subject to review, however, creates a perception that ICT transactions with US firms are inherently risky. Furthermore, the NPRM would impair the ability of US companies to operate in foreign markets, reduce the speed and increase the costs of transactions in the US, and likely make the US a less attractive investment environment.

Below, BSA expands on these concerns and recommends specific revisions to the proposed rules to mitigate them. Though not exhaustive, this constructive critique is intended to focus the Department's attention on concrete solutions to what BSA believes to be the framework's most fundamental weaknesses. To be clear, our concerns are significant, but we do not intend to suggest that the Department should abandon its efforts to implement the Executive Order. To the contrary, in describing our concerns, we seek to provide context for our recommendations, which we believe would result in a framework better suited to achieving the goals of the Executive Order and empower businesses to apply effective supply chain risk management practices consistently and comprehensively.

If these core problems are addressed in a supplemental NPRM, the Department, working together with industry, will be in a better position to address additional details of the proposed rules, including issues on which the NPRM specifically seeks comment.

The Core Problems with the NPRM

The Scope of Transactions Subject to the Proposed Rules Is Too Broad.

The proposed rules are overly – indeed, staggeringly – broad. As written, they would permit the Secretary to launch a review of virtually any "transaction" involving almost any form of commercial technology, regardless of whether it has a clear nexus to national security or to a foreign adversary. Combined with the process and other problems described below, this undefined scope would leave industry in a constant and irremediable state of uncertainty about whether their operations are, or soon will be, subject to regulatory scrutiny.

The most glaring problem concerns the definition of the term "transaction," which reaches beyond expected activities such as acquisitions and transfers to encompass even the mere "dealing in" or "use of" technologies. In concept, these terms could encompass literally any business activity. The NPRM does not define them – in fact, by asking how they should be "best interpreted," the NPRM concedes that the answer is not self-evident.[4] Nor is existing law of much assistance. For instance, the much narrower definition of the "transactions" currently subject to review by the Committee on Foreign Investment in the United States (CFIUS) includes neither of these terms and thus does not shed light on their meaning.

The rules' scope is rendered more unclear by the uncertain identity of "foreign adversaries." Because the NPRM permits the Commerce Department to determine unilaterally and on a case-by-case basis which governmental or nongovernmental entities constitute "foreign adversaries" – without, it should be noted, any formalized guidance or approval from the Department of State or the broader national security community – a company would have no advance notice or predictability about when it might be entering into a transaction subject to this prohibition. Offering transparency around identifying criteria would add sorely needed predictability for US companies. But even after one or more foreign adversaries are identified, uncertainty remains. The proposed rules purport to focus on transactions involving technology "designed, developed, manufactured, or supplied by persons owned by, controlled by, or *subject to the jurisdiction* of a foreign adversary."[5] Because multinational companies – even those domiciled in the US – are "subject to the jurisdiction" of the foreign markets in which they operate, the NPRM could be read to allow the Secretary to prohibit US companies from engaging even in domestic transactions

[4] NPRM, 84 Fed. Reg. at 65318.

[5] NPRM § 7.101(a)(4) (emphasis added).

without the benefit of any due process. In addition, local ICTS purchases within the boundaries of a foreign adversary by a wholly owned affiliate of a US company are at risk because the affiliate would be "subject to the jurisdiction of a foreign adversary."

Finally, the NPRM's effort to constrain the scope of transactions at issue is itself ambiguous. For instance, transactions in which a foreign country or national has an "interest" are a stated focus, but it is unclear what sort of "interest" is of most concern.

The Assessment of Transactions Is Highly Subjective and Unpredictable.

Compounding the problems resulting from the proposed rules' sweeping scope is the highly subjective nature of the Secretary's inquiry. The NPRM authorizes the Secretary of Commerce to block, mitigate, or unwind transactions for technology that pose an "undue risk" of sabotage or subversion to ICT in the United States, an "undue risk" to critical infrastructure or to the digital economy of the United States, *or* an "unacceptable risk" to the national security of the United States.[6] The NPRM provides no guidance about the criteria or standards that the Secretary will use to determine whether a risk is "undue," or "unacceptable," and no criteria on how or when the rules will be applied. Moreover, it is not clear which category of risk is worse, whether "undue" or "unacceptable" is a higher bar, or whether the two terms are synonymous or distinct. The fact that determinations will be made on a "case-by-case" basis adds an element of fluidity to this uncertainty, since a risk that is "undue" or "unacceptable" in one context may not be so in another.

The risks of uncertainty are compounded by the fact that the NPRM outlines no formal process for the Commerce Department to consult with its interagency partners from the Defense and Intelligence Communities that have specific expertise in evaluating supply chain risks. The lack of a formal consultation process heightens the risk that determinations about whether transactions create "undue" or "unacceptable" risks will be made in unpredictable, and potentially inconsistent, manners. Moreover, economic security concerns should not serve as the basis for blocking or unwinding transactions.

Lacking both advance guidance regarding which "risks" the Administration is worried about *and* specificity about the standards that will be used to measure those risks, companies will be unable to perform due diligence assessments to determine whether IT acquisitions may be subject to being blocked, mitigated, or unwound. The challenge is ever greater given the uncertainty about which "transactions" and "foreign adversaries" are of concern and the unavailability of any advanced ruling mechanism to obtain such information.

[6] NPRM § 7.101(a)(5).

The Review Process Lacks Sufficient Transparency and Procedural Safeguards.

The above challenges would be difficult to navigate even if the entire review process were conducted out in the open. But that is not what the NPRM envisions. Instead, the proposed rules keep much of the review process shrouded in secrecy, leaving industry and potentially even government partners in the dark as to what types of transactions warrant concern and scrutiny.

The transparency problem negatively impacts each phase of the entire review process. Under the proposed framework:

- Parties to a transaction are not assured of receiving notice that an investigation is being commenced or of an opportunity (within reasonable time limits) to respond, including when a review is initiated by a private party under proposed Section 7.100(c).
- In contrast, the Secretary is entitled to consult everyone from other designated agency heads to foreign and local governments, meaning that the transaction parties may be among the last to know that they are under investigation.
- Transaction parties are only entitled to receive written notice of a preliminary determination under proposed Section 7.103(a) "when consistent with national security," without any elaboration as to when that precondition is satisfied.
- Although the parties will receive final determinations in writing, only a "summary" will be made publicly available, limiting the value of any precedent that might otherwise guide industry.
- Transaction parties have no right to reconsideration by the Department; the only apparent remedy is a traditional federal court appeal, which may be limited given the deference accorded to agencies on factual determinations related to national security.[7]

In light of this process, it is conceivable that even transaction parties will emerge from a review without a clear understanding of why they were being investigated in the first place and without a practical method of seeking recourse or structuring future transactions. Considering the high economic and reputational stakes associated with an adverse finding – including the onerous compliance burdens and economic and reputational harm for the transaction parties, and the disruption to trade for industry generally – these procedural restrictions are highly concerning.

[7] NPRM § 7.103(h) (noting that a final determination constitutes "final agency action").

The Review Process Lacks Clearly Articulated Standards.

The lack of transparency described above would be a problem even if transaction reviews proceeded pursuant to a set methodology governed by clearly articulated standards, but the NPRM does not set forth such a process.

The NPRM authorizes the Secretary to review a transaction based on the Secretary's sole discretion, at the request of any other government agency, or based upon "information submitted … by a private party," but it does not describe the criteria that will govern the decision to initiate an evaluation. Rather, it only specifies the criteria to be considered once an investigation has been launched.[8] (And, even then, as discussed above, those criteria are fraught with ambiguities.) As a result, there is a significant risk that reviews will occur on an arbitrary basis and that the process could become subject to politicization and/or abuse. Further, the case-by-case nature of the inquiry may not allow for general standards to emerge over time.

As discussed, the quantity of ICT transactions that could be subject to review under the NPRM is enormous. Without stable and predictable understandings of key issues such as what risks are "undue" or "unacceptable" and which transaction partners constitute "foreign adversaries," among other variables, the pace of innovation and trade generally is likely to stall, to the detriment of US industry and consumers.

Recommended Solutions and Revisions to the Proposed Rules

Again, as serious as the above concerns are, the purpose of that discussion is not to suggest that the Department should abandon its efforts to implement the Executive Order, but rather, to issue a supplemental NPRM that provides context for the following recommendations, which BSA maintains would result in a framework better suited to achieving the goals of the Executive Order and the NPRM and would allow for meaningful comments from US industry.

Definitional Changes

As noted, a number of key terms in the proposed rules go entirely undefined. BSA thus recommends that, at a minimum, the following definitions be added to the rules to make them more predictable and better aligned with their intended purpose.

[8] *See generally* NPRM § 7.101.

Regarding the definition of "transaction" (§ 7.2):

- "Dealing in" should be defined – consistent with the definition of "dealer" in Section 3(a)(5) of the Securities Exchange Act of 1934 – as "engaging directly in a financial transaction for the offering, buying, selling, or trading of prohibited ICTS."
- "Use" should be defined as "employing ICTS for its intended purpose," to ensure that it excludes circumstances where an ICTS is used outside the scope of its permitted uses.
- It should be clarified that "transactions" include only inbound transactions.

Regarding the scope of transactions at issue (§ 7.1(a)(2)):

- "Interest" should be defined to limit the scope of reviews to transactions where a foreign entity has a controlling interest in the underlying property. It should exclude de minimis interests, such as a bank financing an entity through a letter of credit or minority or non-controlling interests. Such an exclusion would appropriately narrow the scope of review to circumstances in which a foreign entity has the type of leverage that would be needed to create a potential supply chain risk.

Establishment of Well-Defined Exclusions

To its credit, the NPRM offers one path for better confining its scope, seeking feedback on "classes of persons whose use of ICTS can never violate the Executive Order."[9] BSA would support excluding from regulation entities that meet current and future federal and/or industry-led supply chain security standards, such as:

- Entities that have implemented supply chain security risk management processes that satisfy Section 1323(a)(1) of the ''Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act;"[10] and/or
- Entities whose information processing, storage, or transmission systems meet the standards in NIST Special Publication 800-171 ("Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations");[11]
- Entities whose offerings have been certified as consistent with internationally recognized standards for supply chain practices, such as ISO/IEC 20243; and/or
- Results of DHS ICT SCRM Task Force pertaining to supply chain threat evaluation and attestation frameworks on supply chain risk management best practices.

[9] NPRM, 84 Fed. Reg. at 65318.

[10] https://www.congress.gov/115/bills/hr7327/BILLS-115hr7327enr.pdf.

[11] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf.

In addition, BSA supports exclusions from review for transactions that:

- Have undergone a national security review under another statutory scheme – *e.g.*, ECRA, FIRMMA, or the Team Telecom process at the Federal Communications Commission;
- Involve (i) a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements, or (ii) telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles; [12]
- Only involve personal communications; or,
- Intracompany transactions involving a US-based company and its own foreign subsidiaries.

Additional Procedural Protections and Safeguards

BSA urges the Department to carefully consider the inclusion of safeguards that could help provide industry with greater certainty and ensure that the application of the rules comports with traditional notions of due process. To that end, the Department should consider further rule revisions that would:

- Ensure the process is overseen by an official with adequate levels of political accountability, by amending the definition of "designee" to clarify that the Secretary may only delegate the authorities and duties outlined in the NPRM to an Under Secretary-level designee.
- Eliminate the provisions regarding third party submissions of information to the Secretary under Section 7.100(c).
- Provide a standard for when the Department can invoke Section 7.103(a)'s "national security" exception to forego notifying parties about a preliminary determination. Such a standard should provide a strong presumption in favor of notification which can be overcome only in extraordinary circumstances and only upon notification to Congress.
- Establish a formal interagency process for evaluating whether a transaction presents an "undue" or "unacceptable" risk to ICT supply chains, including a formal determination by the Director of National Intelligence that a transaction, based on available intelligence and other information, represents a threat to US interests.
- Provide explicit protections to ensure business confidential information shared during an investigation is not subject to FOIA/any other public disclosure.
- Provide greater predictability and incentives for proactive industry outreach by establishing a process, modeled on the export control pre-clearance process, for the Department to issue Advisory Opinions. To prevent the Department from being

[12] *See* Section 889 NDAA (Team Telecom).

overwhelmed by requests, the creation of an Advisory Opinions mechanism would necessitate additional clarifications to provide industry with a better sense of the transactions that may be subject to action under the NPRM.
    - For pre-clearance, parties should be able to voluntarily provide advance information on a proposed transaction that Commerce could then elect to review. If Commerce does not elect to review within a specified period, the parties would then move forward with the transaction.
- Provide notice and a chance to respond upon the launch of a review. Reviews should last a minimum of 60 days in order to allow commercial entities to fully participate in the process and to establish potential mitigation methods acceptable to the government.
- Create an independent review process to allow for broader interagency reconsideration of final determinations by the Secretary.
- Commit to Congressional oversight, through:
    - Annual reporting to Congress about the entities deemed (for the purposes of the NPRM) to be a "foreign adversary," and
    - Annual reporting to Congress about the transactions that have been subject to review under the NPRM with safeguards to prevent the disclosure of company-specific information comparable to the current CFIUS process; and,
    - Codification of the suggested procedures, processes, and protections mentioned above.

These revisions will not address all of the problems with the NPRM, but they will go far toward stabilizing the proposed framework and thereby give the Department and industry a sound foundation on which to continue their successful collaboration to date.

* * * * *

We believe in the importance of securing the ICT supply chain and stand ready to work with the Department and other stakeholders to achieve that shared goal.

Sincerely,

Christian Troncoso
Director, Policy