**CHAMBER OF COMMERCE**
**OF THE**
**UNITED STATES OF AMERICA**

January 10, 2019

The Honorable Wilbur L. Ross, Jr.
Secretary
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

**Re: Securing the Information and Communications Technology and Services Supply Chain; 84 FR 65316; Docket No. 191119-0084; RIN: 0605-AA51**

Dear Secretary Ross:

The U.S. Chamber of Commerce (Chamber) respectfully submits the following comments in response to the U.S. Department of Commerce's (Department) request for comment on the proposed rule to implement Executive Order 13873 (EO), Securing the Information and Communications Technology and Services Supply Chain (rulemaking or proposal). This proposal would provide the U.S. government with the authority to intervene in, block, and unwind certain information and communications technology and service (ICTS) transactions on national security grounds.

Our members share the Administration's commitment to protecting ICTS transactions from national security risks. This rulemaking, however, raises significant concerns for a number of reasons, which we detail below.

**First**, the rulemaking would provide the Department with nearly unlimited authority to interfere in virtually any commercial transaction that covers a substantial portion of the U.S. economy. ICTS is ubiquitous in today's economy, found in virtually every type of company in every industry, with thousands of ICTS transactions happening every day. While the Department proposes to pursue a "case-by-case, fact-specific approach intended to avoid overly restricting entire classes of transactions,"[1] this is of little comfort to U.S. companies that would now operate in an environment where *all* ICTS transactions may be subject to review. This could result in significant uncertainty for U.S. businesses, disrupting global supply chains and making investment and sourcing decisions very difficult.

**Second**, the rulemaking does not include substantive measures to provide accountability and transparency. An action taken under this proposal could be extremely damaging to the U.S. economy. Yet the proposal offers little to ensure that the Department fully weighs the ramifications of intervening in a transaction before acting. Further, there is very little in the proposal to help U.S. companies evaluate what ICTS transactions may come under review. This will make it harder for

[1] 84 Fed. Reg. 65316, 65317 (Nov. 27, 2019).

U.S. businesses to enter into relationships with foreign businesses out of fear that these relationships could suddenly and unexpectedly be severed, thereby eroding trust in conducting business with U.S. businesses and marking companies as unreliable.

**Third**, the proposal fails to recognize other national security programs, such as the Bureau of Industry and Security's Entity List or the Committee on Foreign Investment in the United States (CFIUS). National security programs must work in concert with one another to minimize economic harm to an impacted party and build in mitigation measures where appropriate. Otherwise, they may inflict significant harm on U.S. businesses and consumers, all without a corresponding national security benefit. A more deliberate discussion of how this proposal would complement existing programs without overlapping them is necessary.

The Chamber and our members agree with the Department that the ICTS supply chain "is an attractive target for espionage, sabotage, and foreign interference activity."[2] However, securing the ICTS supply chain cannot be done without the U.S. business community's involvement, and this proposal leaves U.S. businesses with little in terms of how to plan around potential threats or evaluate their own efforts (which are often done in coordination with other federal efforts) to secure the ICTS supply chain.[3] This proposal would benefit with greater transparency in the Department's process in evaluating and identifying potential national security threats to the ICTS supply chain.

In light of these concerns, we urge the Department to issue a supplemental notice of proposed rulemaking (SNPRM) before moving to a final rule that provides more detail regarding how it proposes to (1) narrow the scope of covered transactions; (2) ensure accountability and interagency collaboration; (3) provide notice, pre-clearance mechanisms, and reject private party reviews; (4) protect confidentiality in the review process; and (5) define more robust procedures for waivers, appeals, and mitigation.

Below is further discussion of these concerns and areas the Department should examine as it develops this SNPRM.

### *1. The SNPRM Should Narrow the Scope of Covered Transactions*

The SNPRM should narrow the scope of covered transactions. The scope under this proposal is so broad that U.S. companies would not be able to create a predictable compliance program that tracks national security risks determined by the Department. Indeed, the scope of the proposal goes far beyond the Department's traditional jurisdiction over U.S. persons and products, to include persons, products, and transactions that are entirely foreign, including foreign subsidiaries. Despite the stated objective of the EO,[4] this would give the Department the authority to prohibit transactions that occur abroad and involve products and services that are never intended for the U.S.

---

[2] 84 Fed. Reg. 65316 (Nov. 27, 2019).

[3] For example, many U.S. businesses participate in—and follow—recommended standards, frameworks, and regimes that identify good risk management practices in order to facilitate cross-government consistency in improving supply chain security and for increasing clarity about what represents good practice. Examples include the SECURE Technology Act of 2018, adoption of measures to protect sensitive information as documented in NIST 800-171, and adoption of supply chain risk management practices as documented in NIST 800-161 and ISO 20243.

[4] EO 13873, sec. 1.

market, impacting millions of transactions—many of which are already subject to federal review. This would make compliance nearly impossible because of the sheer number of potentially covered transactions. Therefore, clarifying the scope of this proposal is necessary.

Following are examples of transactions that are either low-risk or captured by other federal oversight and should therefore be excluded:

- Sales and services of Commercial Off-The-Shelf (COTS) items (including mass market electronic devices primarily intended for home or small office use).
- Transactions that already are subject to national security oversight by other agencies, or other regulatory regimes, including the CFIUS, Team Telecom, and the Export Control Reform Act (ECRA).
- Transactions where the U.S. party has undertaken threat mitigation efforts as part of their normal risk and compliance program, taking steps to make their networks more resilient to attack through segmentation and encryption.
- Installation and servicing of Local Area Networks (LAN) equipment including routers, switches, network interface cards, and networking cables.
- Internal transactions between a U.S.-based company and its foreign subsidiary (or foreign branch offices).
- Transactions in which the only foreign party is a non-U.S. subsidiary of a U.S. company.
- The provision and servicing of software applications designed for commercial use, including systems software and applications software like operating systems, security software, file management systems, and data processing applications.

This list is not exhaustive, but it illustrates the sheer volume of transactions the proposal could capture if it goes forward as written. The Department needs to clarify what transactions it deems as risks to national security to enable U.S. companies to comply with the proposal.

The Department should clarify the definitions in the SNPRM. The lack of definitions for many of the terms under the proposal exacerbates our concerns over the breadth and lack of notice of what is provided. The Department has specifically asked for assistance in defining the key terms "dealing in" and "use of."[5] First and foremost, these terms—and the rule more broadly—should cover only sales and services provided *by* a foreign adversary to a U.S. entity in the United States. To define "dealing in," the Department could look to the definitions contained in the Securities Act of 1934 for guidance.[6] Under Section 3(a)(5) of the 1934 Act, the term "dealer" means "any person engaged in the business of buying and selling securities … for such person's own account through a broker or otherwise." To borrow from this definition, "dealing in" for purposes of the EO could be defined as "engaging directly in a financial transaction for the offering, buying, selling, or trading of prohibited ICTS provided by a specific foreign adversary that is designated in advance of that transaction." The term "use" could be defined more simply as "employing ICTS provided by a specific foreign adversary that is designated in advance of the transaction for its intended purpose so that unintentional use is not captured. The SNPRM should also provide definitions for the other terms that trigger the prohibition—"acquisition," "importation," "transfer," and "installation." To

[5] *Id.* at 65318.

[6] Codified at 15 U.S.C. § 78c.

the extent that such terms are defined by other regulatory frameworks, we recommend incorporating or referencing such definitions.

The Department should also delete "subject to the jurisdiction or direction of" from proposed § 7.101(a)(4) and revise proposed § 7.101(a)(2) to limit the scope of this authority to transactions in which a "foreign adversary" has an interest and not to "any foreign country or a national" with an "interest" in the transaction or any transaction involving a person "subject to the jurisdiction" of a foreign adversary—which is so broad as to include any individual physically present in the territory of a foreign country. Interests should be defined narrowly to include only current interests that afford the foreign adversary actual physical control or access to ICTS. As discussed above, reviews under this proposal may be extremely disruptive to a U.S. business and any review under this proposal must therefore be tied explicitly to addressing a national security concern.

Additionally, the SNPRM should clarify that transactions that occurred prior to the relevant foreign entity being designated a "foreign adversary" are not subject to review.

The Department should exclude transactions involving ICTS supplied by a party in which the foreign adversary has a minority, non-controlling interest, such as a bank financing an entity through a letter of credit, per proposed § 7.101(b). This would focus the definition of "an interest" narrowly and clarify that the intent is to capture transactions involving ICTS supplied by a party in which a foreign adversary has a controlling interest in voting shares or the ability to appoint a majority of the board.

The SNPRM should also clarify that no party will be held liable under 7 C.F.R. § 7.200 for "causing a violation" or otherwise violating the regulation or any final determination issued under § 7.103 by facilitating a transaction, such as providing transportation services to one or more of the parties of a prohibited transaction, if that party does not have actual knowledge of that prohibition or permission subject to mitigation. With regard to common carriers specifically, the SNPRM should clarify that even if summaries of the Department's final determinations are made public, common carriers and other entities cannot be expected to know whether a particular shipment is part of a transaction that has been prohibited or restricted by the Department, unless it can be demonstrated that it was specifically informed of the prohibition or restriction by the Department or one of the parties of the transaction.

### *2. The SNPRM Should Include Accountability Measures and Interagency Processes*

ICTS supply chain security is a national imperative that requires a whole of government and whole of society approach. Recent actions by this Administration and Congress have included the decision last year to place Huawei and a number of its affiliates on the Bureau of Industry and Security's "Entity List,"[7] the U.S. Department of Homeland Security's establishment of the Information and Communication Technology ("ICT") Task Force,[8] the Federal Communications

[7] Bureau of Industry and Security, "Addition of Entities to the Entity List," 84 FR 22961 (May 21, 2019).
[8] DHS and Private Sector Partners Establish Information and Communications Technology Supply Chain Risk Management Task Force. https://www.dhs.gov/news/2018/10/30/dhs-and-private-sector-partners-establish-information-and-communications-technology

Commission's recent restriction on certain telecommunication equipment in U.S. 5G networks,[9] and Congress' passage of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act, which established the Federal Acquisition Security Council.[10]

*Lack of Whole of Government Approach*

Yet this whole of government approach is not acknowledged in the proposal; indeed, the proposal would allow the Secretary of Commerce (Secretary) to initiate a review that runs contrary to the findings or actions of other federal bodies. For example, the proposal merely requires that the Secretary consult with the heads of specific federal departments and agencies.[11] "Consultation" may be interpreted by government agencies as basic notification, which would reduce the ability of stakeholders in other agencies to analyze transactions or suggest mitigation structures that, from their own perspectives, would alleviate any perceived national security risk. Additionally, nothing in the proposal explicitly limits the Secretary from reviewing a transaction already cleared by another federal agency or body, like CFIUS, potentially subjecting U.S. businesses to multiple, repetitive, time-consuming, costly, and potentially contradictory national security reviews. This potentially overlapping and duplicative process undermines U.S. businesses' credibility to enter into relationships with foreign businesses, hampering their competitiveness and further isolating them in international markets.

The proposal would provide the Secretary with sole discretion to prohibit or mitigate a transaction and assess penalties for violations, without interagency consultation. A process whereby the relevant government agency heads are required to convene for a session or conduct a vote on whether a transaction is subject to the rule or poses a risk to national security, and the appropriate enforcement measures, would ensure that all interested agencies are afforded the opportunity to provide input on key decisions that would impact the critical infrastructure of the United States. Such an approach is similar to how CFIUS conducts reviews involving national security issues, which require that CFIUS voting members include Departmental Secretaries and the Attorney General of the United States.

Intervening with commercial transactions should be a last resort, and only after other options are exhausted. Therefore, we recommend that the SNPRM allow the review to occur only when other legal authorities are not sufficient to address the identified national security risk. [12] Thus,

---

[9] https://docs.fcc.gov/public/attachments/FCC-19-121A1.pdf

[10] Pub. Law 115-390.

[11] Proposed Rule § 7.101.

[12] *See, e.g.*, 50 U.S.C. § 4565 note ("The Committee, or any lead agency acting on behalf of the Committee, may seek to mitigate any national security risk posed by a transaction that is not adequately addressed by other provisions of law" (incorporating Exec. Order 11858, sec. 7)); *id.* § 4565(d)(4)(B) ("The President may exercise the authority conferred by paragraph (1), only if the President finds that … provisions of law, other than this section and the International Emergency Economic Powers Act [50 U.S.C. 1701 et seq.], do not, in the judgment of the President, provide adequate and appropriate authority for the President to protect the national security in the matter"); 31 C.F.R. § 800.101 ("The principal purpose of section 721 is to authorize the President to suspend or prohibit any covered transaction … when provisions of law other than section 721 and [IEEPA], do not, in the judgment of the President, provide adequate and appropriate authority for the President to protect the national security in the matter before the President."); *id.* § 800.501(a) ("The Committee's review or investigation (if necessary) shall examine, as appropriate, whether … [p]rovisions of

a transaction reviewed under the scope of the EO would require the application of positive presumptions to transactions that have already undergone an overlapping or similar review under existing regulatory processes, including those governing CFIUS, section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Section 889),[13] Team Telecom, and the recent FCC restriction on certain telecommunication equipment in U.S. 5G networks. Because many transactions may in fact trigger concurrent reviews under these regimes, coordination and intragovernmental coordination are necessary to serve the interests of all stakeholders, both in industry and in government. Given the overlap in the national security risk issues considered among these multiple processes, a clearance by one process of a specific transaction should preclude review of that same transaction through another national security process. The SNPRM should clarify that such "peer-reviewed" transactions are not subject to subsequent review. This would continue the whole of government approach utilized by the Administration and would provide U.S. businesses with greater regulatory certainty in evaluating potential ICTS transactions. We believe this approach strikes the right balance between protecting national security and preserving U.S. technological leadership.

The proposal includes no explicit requirement that a review under this section be based on credible evidence to support a belief that the transaction in question threatens the national security of the United States. Instead, the Secretary would only need to make a determination that the ICTS transaction in question involves a foreign country and "poses an undue risk" to national security. A requirement of credible evidence is explicitly included in the CFUIS regulations[14] and the SNPRM should include a similar requirement to ensure the Secretary conducts a review where such a threat exists.

The SNPRM should also provide a clear safe harbor for companies that are not directly involved in transactions involving a foreign adversary, and have no knowledge of the technology at issue, which may or may not pose an undue risk to national security. For example, common carriers, freight forwarders, brokers, suppliers, service providers, and other entities using previously provided ICTS in a subsequent transaction that does not involve a foreign adversary. Only those entities directly involved in a transaction with a foreign adversary under review should be subject to prohibitions or restrictions under the proposed rule.

Further, it should be made clear that any penalties issued for violating an order under this EO only be applied if the party is provided notice of the preliminary determination that the transaction is prohibited, given sufficient opportunity to challenge the determination, was given notice of the determination, and knowingly engages in such a transaction following a final determination by the Department.

*Emergency Determinations and Appeals Process*

The SNPRM should eliminate the provision allowing the Department to dispense with the limited process under the rule by declaring an "emergency." Under the current proposal, the Secretary—or his or her "designee"—has virtually no accountability for such a sweeping exercise of

---

law, other than section 721 and [IEEPA], provide adequate and appropriate authority to protect the national security of the United States.").

[13] Pub. L. 115-232.

[14] 31 C.F.R. 800.501(a)(2).

authority, beyond simply including "the basis for the decision" in a final written determination. As drafted, this portion of the proposal would allow an unelected, unconfirmed, and, ultimately, unaccountable official to make ad hoc national security determinations that significantly impact U.S. businesses without sufficient notice or opportunity to challenge such determinations. At a minimum, the SNPRM should provide an appeals process for those notified of a decision under the emergency authority of § 7.104 to provide an impacted entity the opportunity to respond and mitigate going forward.

*Foreign Adversary*

The SNPRM should more specifically define a "foreign adversary." The rulemaking proposes to make transactions involving ICTS "designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary,"[15] with a "foreign adversary" defined as "any foreign government or foreign non-government person determined by the Secretary to have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States."[16] This provides significant latitude to the Secretary, and more clarity is needed. We provide recommendations below to improve clarity.

**First**, the definition of "foreign adversary" needs to be revised. The list of transactions discussed in the section on scope of transactions above illustrates the sheer number of transactions that may fall under review, especially if a foreign adversary is a government. One approach would be to include *only* specific foreign non-government persons, not foreign governments. By including "foreign governments" in the definition of "foreign adversary," the current proposal threatens to capture transactions with *any* entity in a designated country—including transactions with non-U.S. subsidiaries of U.S. companies in those countries. If the definition of "foreign adversary" were implemented in its current form, it would inflict direct harm upon the U.S. parent companies of those non-U.S. subsidiaries by treating the subsidiaries themselves as if they are foreign adversaries. Should the Department continue including "foreign governments" in the definition, the SNPRM should exclude governments that are long standing allies of the U.S., like NATO and major non-NATO allies.

**Second**, the SNPRM must require that specific foreign adversary entities be designated in advance of any transaction subject to review. If a party to a transaction is designated after the transaction has been initiated under a legally binding agreement, the transaction should not be reviewable under the rule. To allow otherwise would threaten the finality of all U.S. companies' transactions and would discourage business with those companies.

**Third**, the SNPRM should provide for a specific, transaction-based list on which foreign adversaries will be named, and that list should specify which transactions with each listed entity are reviewable under the rule. The Export Administration Regulations' Entity List, which imposes targeted restrictions with regard to specifically listed entities, is a useful model that could be applied here.

[15] *See* Proposed § 7.101(a)(4).
[16] *See* Proposed § 7.2.

*Accountability*

The proposal intends to grant a wide scope of authority to the Department and it is imperative that the ultimate decision-maker be accountable politically. As drafted, the proposal would allow the Secretary to assign decision making authority to a "designee."[17] We recommend that the delegation be restricted to a designee who is subject to Senate confirmation, preferably no lower than the Deputy Secretary. This will ensure that Congress can hold the executive branch accountable for enforcement actions under the EO, including by holding hearings and submitting requests for information. The rule must also provide specificity as to how this will be implemented, and which agency, bureau, or office within the Department would have authority and oversight.

The SNPRM should include a requirement that the Department publish an annual report in the *Federal Register* on the number of transactions reviewed, blocked, and mitigated, but that does not disclose the names of the parties involved—similar to reporting in the CFIUS process. The report should also describe, on an unclassified basis, and without revealing party names, the category of ICTS involved and the national security rationale for the Department's actions in each case in order to provide notice to those in the ICTS community on areas of enforcement.

### *3. The SNPRM Should Provide Notice and Pre-Clearance Mechanisms and Reject Private Party Reviews*

The proposal allows the Department to commence a review at any point, even after a transaction has closed, and provides no opportunity for parties to request an advisory opinion or pre-approval for a contemplated transaction. Coupled with the refusal to offer "advisory opinions,"[18] this structure creates significant uncertainty. The SNPRM should provide a voluntary pre-clearance process, similar to that in CFIUS, where parties can notify the Department of transactions involving foreign adversaries and receive a ruling prior to consummating the transaction. If the Department does not respond within a reasonable period of time, parties to the transaction should be permitted to proceed within a safe harbor.

*Notices and Proposed Timelines*

The current proposal does not provide a party with a meaningful opportunity to respond to any action the Department proposes, including the opportunity to present business confidential information. The proposed 30-day timeline to respond to a preliminary determination is too short and does not provide parties with sufficient opportunity to engage with the Department, including, for example, to propose mitigation.[19] The Department should consider adopting a minimum of 60 days for the post-notification response period and review process to allow commercial entities the ability to fully participate in the process and establish potential mitigation methods acceptable to the government. At the same time, stricter enforcement methods for governmental timelines serve as important forcing functions to ensure efficient and accountable decision making. As drafted, the proposal would allow the Secretary to hold parties to an unreasonably short 30-day submission

[17] *E.g.*, Proposed Rule § 7.2 (defining "Secretary" as "the Secretary of Commerce or the Secretary's designee").
[18] Proposed Rule § 7.7.
[19] *See* Proposed § 7.103(a).

deadline, but then it extends the government's own review indefinitely, subject only to "the Secretary [sic] discretion."[20]

By way of comparison, the recent revisions to the CFIUS process sustain (and actually extend) the timeframes for analysis of proposed transactions, including 45-day review periods and 45-day investigations, if appropriate.[21] Such 45-day review periods are in addition to and follow an initial voluntary notice period, which provides parties to a transaction time to present information to the agency and begin developing a mitigation plan. The Department's own Export Administration Regulations offer other potential models. They provide several months of time to engage with government stakeholders following notice that the government intends to deny an export license application:

> You will be allowed 20 days from the date of the notification to respond to the decision before the license application is denied. If you respond to the notification, BIS will advise you if, as a result of your response, the decision to deny has been changed. Unless you are so advised by the 45th day after the date of the notification, the denial will become final, without further notice. You will then have 45 days from the date of final denial to exercise the right to appeal under part 756 of the EAR.[22]

This allows for a combined total of 65 days for parties to engage with the government, as well as three opportunities that include an appeals process, compared with the 30 days and no opportunity to appeal as set forth in the proposal. Importantly, the "intent to deny" itself must include a statement about "[w]hat, if any, modifications or restrictions to the license application would allow BIS to reconsider the license application."[23] Similar provisions and procedural clarity would be valuable in this instance.

In addition to the notice deficiencies described, the proposed review process is problematic because the Secretary need only give notice of a preliminary determination "when consistent with national security."[24] The SNPRM needs to provide guidance on how that determination will be made to ensure decisions are not wholly discretionary. The Secretary's discretion to withhold notice should be limited.

*Information Submitted by Private Parties*

The Department should reject the option to initiate a review based on information submitted by private parties.[25] This mechanism would invite abuse by other companies attempting to discredit rivals to gain an unfair advantage in the marketplace. Moreover, while companies may be subject to obligations to submit accurate information to the government under existing statutes,

---

[20] *See* Proposed § 7.103(j).
[21] Provisions Pertaining to Certain Investments in the United States by Foreign Persons Proposed Regulations, 84 Fed. Reg. 50174, 50204 (Sept. 24, 2019) (proposing new timing rules at 31 C.F.R. § 800.503-508).
[22] 15 C.F.R. § 750.6(b).
[23] *Id.* 750.6(a)(4).
[24] *See* Proposed § 7.103.
[25] 84 Fed. Reg. 65321 (Nov. 27, 2019) (Section 7.100(c).

such as the False Statements Act,[26] without the ability of a company to respond to information that has been submitted by a third party, it may be difficult for the U.S. government to assess the accuracy and completeness of the information it has received or understand if that information is false or misleading. All of this would require the Department to dedicate significant resources to investigate and resolve all of these reports, which would detract from the Department's ability to provide timely and fair reviews of transactions that do warrant review—further stringing along and de-legitimizing U.S. businesses. The private party submission mechanism therefore should be eliminated from the next iteration of the proposed rule.

### *4. The SNPRM Should Propose Procedures to Protect Confidentiality*

The proposal states that the Secretary may consider business confidential or proprietary information as part of the evaluation of a transaction subject to the EO. However, the proposal contains no protections to shield sensitive proprietary or trade secret data from external review. Accordingly, the public likely would be able to access such data or information through the FOIA process, or potentially following the Secretary's publication of information summarizing decisions in the *Federal Register*.[27]

U.S. businesses need to be assured that their information will be kept confidential. The SNPRM should explicitly describe procedures to protect business confidential information that is submitted to the Department by parties subject to reviews and seek congressional authority to protect such information if necessary. This would help ensure that parties have a meaningful opportunity to engage with the Department without the risk that exposing business confidential information submitted as part of the process would become public. Such procedures for CFIUS review are statutorily granted, and the Department should consider requesting similar protections from Congress with regard to the EO.[28]

In the interim, the Department should consider publishing detailed reports only to the extent necessary, and only for those transactions that result in blocking or unwinding a transaction. In no instance should the Department publish the name of a company to a transaction as this could be highly prejudicial, particularly if a company has or is planning to mitigate. As in the CFIUS context, mitigated transactions should not be public. Public reporting should provide only categories of ICTS and not provide any identifying information for the entities involved. Adopting these practices will encourage more effective functioning of the review process.

### *5. The SNPRM Should Propose Waiver and Mitigation Processes*

The proposal contains no categorical waivers or exceptions, stating:

---

[26] *See* 18 U.S.C. § 1001(a) ("Except as otherwise provided in this section, whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully—(1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact; (2) makes any materially false, fictitious, or fraudulent statement or representation; or (3) makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry; shall be fined….").

[27] Proposed § 7.6, 7.103(i).

[28] *Cf.* 50 U.S.C. § 4565(c), (g).

> The Secretary has declined to identify classes of transactions that are subject to prohibition or are excluded from prohibition. Determination of transactions prohibited by the Executive order will be made on a case-by-case basis. Should the Secretary determine based on a particular case that a class of transactions should be prohibited or excluded, the Secretary will publish such determination and further guidance or request for comment (if needed) in the *Federal Register*.

Like this proposal, Section 889 regulates security reviews of telecommunications equipment and services.[29] Unlike the proposal, however, Section 889 provides two statutory exclusions: (1) a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or (2) 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. The SNPRM should incorporate these same exceptions.

Section 889 also establishes a delayed implementation "waiver" process where impacted entities can work with the U.S. government to develop a mitigation plan to resolve issues identified through the disclosure process. As discussed, when the Department identifies a material risk, it should impose mitigation rather than blocking the transaction whenever possible (and, in any event, should only take action if it determines that no other legal authorities are available to address a national security risk arising from a transaction).

The Department should also incorporate into the SNPRM a requirement that the Secretary take into account as part of any decision in this proposal other cost-benefit analyses—practicability, economic cost or harm, safety, availability of alternative technologies, effect on product planning and development cycles, and other factors to ensure that a prohibition or mitigation plan is appropriately tailored to the circumstance and minimizes the risk of unintended economic or security consequences.

Further, the Department should adopt a standard of "reasonable care" where companies that follow industry best practice standards for due diligence and care in the evaluation of goods and services should be given some level of deference for good faith and not be penalized for transactions that were reasonably believed to be outside the scope of the law regardless of any opposing final agency determination. Both CBP and IRS have adopted similar standards, and these standards should be incorporated into this proposal.

Such a mitigation process should include certain elements to ensure meaningful exchanges of information between industry and government. These elements include defined, predictable timelines for review of mitigation; a defined process for review by the Department and interagency partners; and a fundamental preference for mitigation over prohibition.

The Department should consider a more proactive approach to examining classes of transactions based on the case-by-case review. The proposal leaves open the possibility that the Secretary can make a categorical determination to prohibit or exclude transactions based on specific cases, but it does not provide a clear process for when or how such a determination would be considered. The Department should include in the SNPRM a requirement, rather than an option,

[29] Pub. L. 115-232.

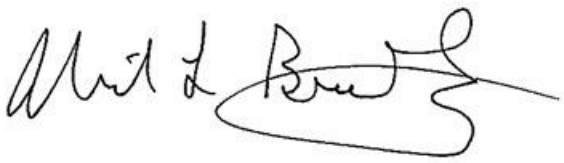
that any determination on a specific case be evaluated for potential applicability to an entire class of transactions. This should be done under a standard rulemaking, with opportunity for comment. The Department's determination based on any such review should be public and include a clear justification of the Department's decision to the extent possible without compromising confidentiality or security.

The Department need not design out of whole cloth the process outlined in the proposal. As discussed, certain elements of the SNPRM should be modeled on the CFIUS process, which provides a detailed, efficient, and proven approach to protecting national security while fostering efficient investment decisions. It could also look to the streamlined licensing process at the Bureau of Industry and Security for the SNPRM's advanced approval mechanism process. Both of these examples allow industry and government to engage in meaningful dialogue, giving the government more nuanced insight into the proposed transaction and ensuring that the parties to the transaction understand what national security bounding conditions would apply in a given set of circumstances. These structures, and the associated confidentiality protections, provide essential certainty and clarity for all stakeholders. The Department should consider such approaches as it develops the SNPRM.

***Conclusion***

Thank you for the opportunity to comment on the Department's proposal. While our members share the Administration's priority to secure ICTS transactions, this rulemaking proposes to provide the Secretary with significant authority to intervene in, block, and unwind essentially *any* ICTS transaction, with little to no accountability, transparency, or coordination with other government programs. This could result in significant harm to the U.S. economy, businesses, and consumers without a corresponding national security benefit. We therefore strongly urge the Department to issue a SNPRM that responds to the concerns discussed above. We look forward to continuing to work with the Department—and other federal agencies—to help solve the critical challenges in securing the supply chain.

Sincerely,



Neil L. Bradley
Executive Vice President
and Chief Policy Officer

Christopher D. Roberti
Chief of Staff and Senior Vice President,
Cyber, Intelligence, and Security

cc:

Steven Mnuchin, Secretary, U.S. Department of Treasury
Cordell Hull, Acting Deputy Under Secretary, Bureau of Industry and Security

Richard Ashooh, Assistant Secretary of Commerce for Export Administration, Bureau of Industry and Security
Douglas Kinkoph, Acting Assistant Secretary, National Telecommunications and Information Administration
Henry Young, Senior Technology Policy Advisor, U.S. Department of Commerce