ITI Promoting Innovation Worldwide

Mr. Henry Young
U.S. Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

January 10, 2020

RE: ITI Comments Responding to Commerce Dept. Notice of Proposed Rulemaking on Securing the Information and Communications Technology Supply Chain (DOC-2019-0005; RIN 0605-AA51; 84 FR 65316)

Dear Mr. Young:

The Information Technology Industry Council (ITI) welcomes the opportunity to comment on the Department of Commerce's Notice of Proposed Rulemaking (NPRM) – hereinafter the "NPRM" or "rule" -- on Securing the Information and Communications Technology Supply Chain.

ITI represents the world's leading information and communications technology (ICT) companies. We promote innovation worldwide, serving as the ICT industry's premier advocate and thought leader in the United States and around the globe. ITI's membership comprises top innovation companies from all corners of the technology sector, including hardware, software, digital services, semiconductor, network equipment, and other internet and technology-enabled companies that rely on ICT to evolve their businesses.

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 industry has devoted significant resources, including expertise, initiative, and investment in cybersecurity 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 obligation to address risks to global information and communications technology supply chains and national security more broadly. We believe government and industry must work together to achieve the trusted, secure, and reliable global supply chain that is a necessary priority for protecting national security and an indispensable building block for supporting innovation and economic growth.

It is through this lens through which ITI offers our comments in response to the NPRM, which focus principally on the following: (1) general principles to guide Commerce as it seeks to implement the underlying Executive Order 18373 (hereinafter "the EO"); (2)

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

clarifying several foundational definitions; (3) the process and criteria for evaluating transactions; (4) providing a roadmap for a more specific, focused implementation of tahe EO; and (5) addressing the questions posed in the NPRM.

That the balance of our comments are intended to provide constructive advice should not obscure the fact that the proposed Rule, as written, is fundamentally flawed in several respects. Nothing less than a very significant reconsideration of both substance and process will render such a rule workable or effective in terms of American national security, U.S. economic competitiveness, or overall due process. Immediately below we offer several overarching comments in this regard.

The business community is an indispensable partner to any Commerce efforts to rationally implement the EO and needs ample time to provide helpful feedback., ITI appreciates the Commerce Department's decision to publish these measures as an NPRM as opposed to an Interim Final Rule, as doing so maximizes the ability of the business community to provide critical feedback to the Department as it seeks to tailor the implementing measures to the national security imperatives underlying Executive Order 18373. ITI is disappointed, however, in the expedited timeframe for providing comments, particularly with respect to a rule with such vast legal scope and economic implications. Moreover, because this NPRM provides almost no specifics, industry cannot meaningfully comment on it. As such, we would ask that any further rulemaking is issued in the form of a detailed Supplemental Notice of Proposed Rulemaking (SNPRM) and provides industry with sufficient time to consult, review proposed changes and provide feedback.

The scope and breadth of the proposed Rule is alarming and unnecessarily undermines all information and communications technology and services (ICTS) transactions with any nexus to the U.S. The NPRM as drafted is too broad to be practically implementable and goes well beyond that which is necessary to protect national security and prevent undue security risks to critical infrastructure supply chains. As a result, the NPRM unnecessarily casts a cloud of uncertainty over all ICTS transactions with any nexus to the United States, including those that present no or low risks to national security.

The proposed Rule is overbroad and too vague for companies to practically comply with, raising significant due process concerns. While we are encouraged that the Commerce Department has attempted to take a risk-informed, technology-neutral, case-by-case approach grounded in specific, factual information, including as it relates to potential mitigations, the scope of the NPRM as currently drafted is far too vague, overbroad, and replete with unknowns for our member companies to possibly understand how they would comply with such a regime. As such, the NPRM provides inadequate notice and raises significant concerns regarding due process and fairness which must be remedied in further iterations of the Rule.

The proposed Rule appears to be untethered from the requisite national security criteria in the EO, and thus ultimately won't adequately address such risks. The EO empowers the Secretary of Commerce to block ICTS transactions only when such transactions involve a clear connection to a foreign adversary and pose unacceptable risks to national security or

undue risks to critical infrastructure or the digital economy. However, the proposed Rule outlines a regulatory regime that appears to gloss over these fundamental threshold requirements. We support regulations, laws, and measures that are calibrated to, based in factual evidence regarding, and focused on addressing identifiable national security risks. While the EO articulates such specific requirements, the proposed Rule does not; these flaws must be remedied to meet the national security objectives underlying the EO.

The proposed Rule creates an unacceptable level of business uncertainty, threatening to undermine the competitiveness and technological leadership of U.S. companies. While the questions posed in the NPRM appear designed to elicit input on how to rationally narrow the rule, many additional questions remain about how the evaluation process set forth in the NPRM will commence and function in practice. Lack of clarity in scope and process makes for an uncertain business environment and threatens the ability of companies to compete with foreign companies not subject to U.S. or similar foreign conditions. Overbroad policy approaches, such as embodied in the proposed Rule, stifle U.S. innovation, technological leadership, and competitiveness. Commerce and other U.S. policymakers should seize the opportunity to advance supply chain policy approaches that are not only compatible with but drive global policymaking norms.

Unless the Rule is fundamentally reexamined and more appropriately calibrated to address the above concerns, it could do lasting harm to the United States' global technological leadership. The broad scope and unlimited discretion granted to the Secretary of Commerce (hereinafter, "Secretary") means that virtually all interactions between companies' U.S. operations and the rest of the world risk review. That may make partners outside of the U.S. hesitant to enter into relationships with companies for fear that those relationships could suddenly and unexpectedly be severed, eroding trust in buying from U.S. suppliers and making U.S. companies appear as unreliable business partners. The outcome could be a U.S. technology sector isolated from the world.

1. General Principles

We encourage the Commerce Department to consider the below guiding principles in developing a Rule to implement the Executive Order and ensure the security of the ICTS supply chain.

- **The Rule should be used to advance and protect U.S. national security objectives without putting American competitiveness at risk or eroding trust in American or allied country companies as partners.** U.S. competitiveness and commercial success depend upon regulatory certainty and clarity. The NPRM fails to deliver this certainty, as it provides no way for U.S. or foreign persons to know which types of goods, services, technologies, people, or business activities could trigger the government's review and potentially lead to a decision by the Secretary to block, alter, or order the unwinding of a transaction at any time after it has been completed. This, in turn, may make foreign businesses less likely to do business with U.S. companies since, for reasons they can never know and without meaningful judicial review, the U.S. government could decide to nullify completed

transactions, imposing additional costs on parties to ICTS transactions. This will directly harm the competitiveness U.S. ICTS and related industries, thus undermining overall U.S. national security.

- **The Rule should address only identifiable, material concrete national security risks for a narrow subset of ICTS elements.** These risks should, at a minimum, be directly tied to actionable threats identified by the Office of the Director of National Intelligence (ODNI) or other threat information that the U.S. government possesses.
- **The Rule should provide clear guidance to industry by including parameters and criteria for a fair, workable, and repeatable process that Commerce will use when evaluating transactions.**
- **The Rule should not apply if other existing U.S. legal authorities are available.** There are currently several other national security review mechanisms in place, including the Committee on Foreign Investment in the United States (CFIUS) process, the recent FCC restriction on funding for telecommunications equipment, Section 889 of the 2019 National Defense Authorization Act (Section 889), Team Telecom, and the Export Administration Regulations (EAR). Any new authority should be coordinated with all of these established processes to ensure transactions are not covered under multiple review mechanisms. The proposed rule should only provide new authority in areas not already covered by existing regimes.
- **The Rule should seek to evaluate only pending or future transactions; looking backwards to potentially reopen closed transactions diminishes business certainty and raises legal questions.**
- **The Rule should be guided by existing taxonomies to incorporate sufficient and clear processes for interagency review, notice and due process.** For example, Commerce should look to interagency review processes that are well-established in existing statutes, such as the EAR and CFIUS, including provisions of ECRA and FIRRMA from the FY2019 NDAA. Commerce could also look to existing regimes as a guide to narrowly tailor review of transactions to only those specific items that raise national security concerns.
- **Clear and consistent guidance should be provided across different parts of the Rule.** At present, the way the NPRM is written is confusing and there are instances when one part of the NPRM provides guidance that is not consistent with another part. For example, § 7.103 describes rules for written determinations, and indicates the Secretary will provide notice to parties "when consistent with national security." However, Section II of the NPRM indicates the Secretary will provide notice to parties "as appropriate." Neither term provides an adequate level of clarity. ITI recommends ensuring that language and guidance is consistent across the Rule.
- **The Rule should provide sufficient protection for confidential and/or proprietary business information.**

- **The Rule should not include transactions for personal services.** Commerce should clarify that covered services under this rule do not include personal services, such as those provided by engineers.
- **Measures should be incorporated to ensure the Secretary is accountable.** The Secretary should not be able to assign final decision-making authority to a "designee" at any level lower than a Senate-confirmed Assistant Secretary. This will ensure that Congress can hold the executive branch accountable for enforcement actions, including by holding hearings and submitting requests for information from political appointees. The Rule should also lay out a formal interagency process to initiate the review of a transaction.

2. Definitions

The Executive Order grants the Secretary the authority to prohibit any acquisition, importation, transfer, installation, dealing in, or use of (a "transaction") information and communications technology or service subject to US jurisdiction. While the NPRM uses the same definitions for both "ICTS" and "transactions" as used in the EO, it is critical that an eventual final Rule clearly define these and other key terms, as identified below.

Transaction: As currently defined, transaction ostensibly captures every single activity undertaken by a company – in other words, the constant motion of companies' business activities. The terms "transactions" and each of the illustrative terms comprising the definition itself must be clearly defined in a manner that rationally helps achieve the national security imperative at the core of the EO and NPRM. By clarifying these terms, companies would have notice of the types of commercial activity that may be subject to additional scrutiny.

One approach to defining what elements of "transactions" are covered would be to eliminate the illustrative terms that are either redundant with the term "transaction" itself or that are so vague as to only introduce confusion – such as "dealing in" and "use." Instead, Commerce should clearly articulate what commercial activities are not intended to be captured. For example, broad terms such as "dealing in" seem to clearly capture all manner of transactions, including export and investment transactions that are likely covered under other regimes. We recommend the Department carefully delineate which transactions cannot be considered in scope by employing an approach that embraces principles of statutory interpretation.

We recommend additional clarification by defining the other terms that can trigger the prohibition of a transaction – "acquisition," "importation," "transfer," and "installation." To the extent such terms are defined by other regulatory frameworks, we recommend incorporating or referencing such definitions. We also recommend further clarifying these terms as limited to covering transactions that are clearly subject to U.S. jurisdiction and not covered by other national security review mechanisms. For example, export transactions should be out of scope because they are covered by the EAR, investment transactions should be considered as out of scope because they are covered by CFIUS, etc.

Interest: Commerce should further define what "an interest" means with regards to the element of "property in which any foreign country or national thereof has an interest." As written, the language is overbroad and would capture transactions in which a foreign person has only a tangential, non-controlling interest. To align with the national security objectives, Commerce should revise this definition to only apply where there is a nexus to a "foreign adversary." At a minimum, an exclusion should be provided for de minimis interests, such as a bank financing an entity through a letter of credit or minority or non-controlling interests. This would focus the definition of "an interest" narrowly and clarify the intent as to capture majority or controlling interests.

Foreign adversary: Commerce should revise the definition of foreign adversary to foreign adversary *person,* which means any foreign non-government person[1] determined by the Secretary to (1) be owned by, controlled by, or subject to the direction or influence of a foreign adversary government entity and (2) have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons for the purposes of Executive Order 13783.

Jurisdiction: Commerce should also clarify the term "subject to jurisdiction" throughout the rule. Neither "subject to jurisdiction" nor "subject to the jurisdiction of a foreign adversary" are defined and should be defined narrowly in a SNPRM. For example, under the EAR, non-US transactions can trigger a review, and if a similar interpretation is adopted here, the result could be to capture many transactions with no significant nexus to U.S. national security interests. ITI recommends that Commerce better limit the definition of "subject to U.S. jurisdiction" to mean transactions in which the subject ICTS is used in the territory of the United States. ITI also recommends that this definition clarify that it does not capture a multinational's internal transactions between its U.S. and foreign operations, or transactions between a U.S. entity and foreign subsidiaries of other U.S. companies where neither party to the transaction has a nexus to a foreign adversary.

3. Process & Criteria for Evaluating Transactions

The NPRM lays out three steps by which the Secretary would evaluate transactions, but those descriptions are concerningly vague and require significant further clarification. ITI recommends that Commerce addresses the following areas:

A. The process to initiate a review of a transaction is vague

The process by which the Secretary will initiate a review of a transaction, including to consult with other agency heads to determine whether a transaction should be evaluated, lacks clear parameters and should be clarified.

Regarding the consultative interagency process, it is not clear whether this would be an ad-hoc engagement every time a potential transaction falls within the scope of this authority

[1] "Person" is defined in §7.2 of the proposed rules as "an individual or entity," and "entity" is defined as "a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization."

or whether it will be a more formal process. ITI recommends establishing a more formal interagency vetting process to evaluate transactions, requiring all agencies to provide input on key decisions regarding whether a transaction is a) in scope and b) presents a national security risk to the United States. We recommend Commerce first look to existing interagency bodies, such as CFIUS, and establish a similar, formal interagency group here.

The processes by which the Secretary may initiate review of a transaction by his own volition, or by which private parties may submit information regarding a transaction to launch a review, are equally vague. Companies would have no idea whether they would ever be safe from review, and further, the lack of guidance regarding the process for private parties to submit information could incentivize self-interested behavior.

Regarding the Secretary's review of transactions and enforcement action *sua sponte*, the NPRM as currently written vests the Secretary with seemingly boundless discretion, which casts a shadow of uncertainty over all transactions involving ICTS. A formal interagency process, including convening a session or establishing consensus on whether a transaction is subject to the Rule, as outlined above, would provide a holistic government view, as would be appropriate where the government is weighing whether to intervene in dealings between private parties.

Regarding the commencement of investigations based on information submitted by private parties, the NPRM provides almost no information regarding how such a process might work other than that the information submitted should be by "credible" private parties. This seems to open the door for potentially nefarious, commercially self-interested behavior to occur. ITI recommends removing this process altogether. However, should Commerce decide to retain the private party referral provision, Commerce should establish clear guardrails to ensure fairness and address due process considerations. If Commerce retains the concept of a private party referral process, we additionally recommend that Commerce include specific questions regarding such a process in a SNPRM.

B. Criteria to trigger a review of a transaction is inconsistent with the Executive Order

The criteria to trigger a review of a transaction as laid out in the NPRM are all-encompassing and appears to be even broader than the criteria laid out in the Executive Order. The Executive Order prohibits transactions that a) involve ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary and b) pose an undue risk of sabotage or subversion to ICTS in the U.S., or pose an undue risk of catastrophic effects on the critical infrastructure or the digital economy, or otherwise pose an unacceptable risk to national security.[2]

By contrast, Section 7.101(a) of the Rule provides that the transaction may be subject to evaluation if it is: (1) conducted by U.S. persons or involves property subject to U.S.

[2] Executive Order 13873, 84 FR 22689 (May 15, 2019).

jurisdiction; (2) involves any property in which a foreign country or national has an interest; and (3) was initiated or completed after May 15, 2019; (4) involves ICTS tied to a foreign adversary; and (5) poses risks to national security, critical infrastructure, or the digital economy.

Without further guidance, it appears that every U.S. technology transaction involving an international business partner could trigger a review under this Rule – even those that do not create any risks at all. As noted above, including review of all transactions where there is simply a "foreign interest" is overbroad. We urge the Commerce Department to avoid considering all foreign transactions as potentially in scope, but rather only those that involve specific risk, as all foreign transactions are not inherently risky.

C. Process considerations regarding notifying parties and issuing determinations

Transparency and due process are essential to business certainty and competitiveness. The NPRM as written only requires the Secretary to provide notice to parties "when consistent with national security" or "as appropriate," terms that seem to be left wholly up to the discretion of the Secretary or his designee. It also remains unclear whether parties to a transaction will always be given notice or whether they will only be given notice "as appropriate." ITI urges the Secretary to always immediately provide direct notice to parties that a transaction they are party to is being evaluated. Such direct notice should include information regarding the basic facts of the transaction so that companies know what is being evaluated.

While we appreciate the NPRM provides parties with the ability to submit opposing information demonstrating how an identified risk might be mitigated, providing ample time to parties to assemble that information or establish appropriate mitigation mechanisms is critical. The current 30-day timeline in the NPRM is too short; we recommend that Commerce allow for a 60-day post-notification response period for parties to fully participate in the process and establish potential mitigation methods acceptable to the U.S. government. Commerce's Export Administration Regulations (EAR) offer a potential model to consider, as the EAR provides for a response window of 65 days, including three opportunities to respond to and appeal the process.[3]

Third, we have questions about the process by which the Secretary would make a final determination public. The phrase "as appropriate" is used again here, and it is not clear when or under what circumstances the Secretary would make such a determination public. While it would be helpful for Commerce to provide some information regarding the types of transactions it has reviewed and the results, further public disclosure of the names of involved parties could cause substantial economic and reputational harm to U.S. businesses, even where mitigation mechanisms are available and have been employed to address any perceived risks. Thus, ITI urges Commerce only to publish information that would not directly or indirectly reveal the names of the parties to the transactions, other than the names of parties who have been designated as foreign adversaries. For

[3] See 15 C.F.R. § 750.6(b).

information other than party names, ITI recommends that, at a minimum, the release of such information follow the FOIA process and thus, that typical exemptions from FOIA apply to this information as well.

Relatedly, the NPRM allows the Secretary to consider business confidential or proprietary information as a part of the evaluation of a transaction. However, the NPRM contains no protections to shield sensitive proprietary or trade secret data from external review or access. In order to fully participate in the review and potential mitigation process, businesses need to be assured their information will be kept confidential. The rule should explicitly describe procedures to protect business confidential information. Such procedures for CFIUS review process purposes are statutorily granted, and Commerce may consider requesting a similar protection from Congress with regard to Executive Order 13873.[4]

D. Process considerations regarding emergency procedures

The NPRM gives the Secretary the ability to bypass all procedures set forth in the rule should "public harm [be] likely to occur" in the process of following the procedure or should "national security interests require it."[5] As an initial matter, we question whether this level of broad, emergency discretionary authority is ever appropriate, particularly in light of the substantial authorities already otherwise granted under the rule. At a minimum, the Department should clarify what types of circumstances it contemplates as giving rise to the necessity for the Secretary to exercise such powers. Additionally, the exercise of such broad discretionary authority, without explanation, gives rise to due process concerns. This section needs to be more narrowly scoped and nuanced to ensure that the "regular" process is only disregarded in the most egregious national security circumstances and so that it requires interagency agreement, therefore avoiding violating the due process rights of parties. In addition, where the Secretary considers it necessary to dispense with these procedures, the final determination should include an explanation of the particular circumstances justifying this approach. We also strongly recommend including language in the rule to prevent this authority from being delegated under any circumstances.

E. Assessing the "effect" of a transaction

We urge the Commerce Department to clearly articulate the criteria that are used to assess the "effect" of a particular transaction, which in our view should be clearly related to the actual national security risk posed by the transaction. As such these criteria should be focused on addressing acute national security risks to the United States and should not include trade policy or other commercial concerns.

In assessing the actual national security risk posed by a transaction, one of the evaluation criteria the Secretary is directed to consider is whether the transaction involves "ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or

[4] *Cf.* 50 U.S.C. § 4565(c), (g).
[5] Proposed Rule § 7.104.

subject to the jurisdiction of or direction of, a foreign adversary."[6] First, as mentioned previously, in ITI's view only "persons," not countries, should be designated as foreign adversaries (see, infra, p.6). If Commerce adheres to this recommendation, then the phrase "subject to the jurisdiction of" should be deleted as moot, given that entities cannot be subject to the jurisdiction of "persons" (whether they are foreign adversaries or not).

Second, even if Commerce rejects our proposal to limit the designation of foreign adversaries to "persons," ITI still maintains the phrase "subject to the jurisdiction of" should be deleted for the following reason. Ostensibly any company operating in a nation considered to be a foreign adversary would be subject to the laws (and hence jurisdiction) of that country, just as a foreign company operating in the U.S. would be subject to U.S. laws. Therefore, being subject to the jurisdiction of a country designated as a foreign adversary is overbroad and should not be a decisive factor in triggering a review, as it is a potentially meaningless designation in the context of companies doing business globally.

The Department should delete the reference to "jurisdiction" and clarify that its intent is to focus on transactions involving companies that have been designated as foreign adversaries, or entities where foreign adversaries have a majority or controlling interest, and not designate countries as foreign adversaries at all, as articulated above.

4. Establishing a Roadmap for More Specific Implementation

Given that the scope of the rule is so broad and there are no parameters of what is or is not included, we urge the Commerce Department to dramatically narrow and significantly clarify the scope of transactions that it would consider to present identifiable and concrete risks, based on specific and verifiable threat and vulnerability information, and to provide more clarity on who or what is considered to be a foreign adversary. In order to rationally shape this rule and make this authority as targeted as possible, ITI offers the following suggestions:

A. Designating Foreign Adversaries

Because the designation of one or more "foreign adversaries" is a necessary prerequisite for the Secretary to exercise his authority to prohibit, block, or unwind, any ICTS transaction pursuant to the EO, the designation of one or more foreign adversaries is a key threshold criterion that must be satisfied prior to determining whether a nexus to a foreign adversary exists. However, as drafted, the NPRM does not establish any process by which foreign adversaries will be so designated nor identify any foreign adversaries. We urge the Commerce Department to establish a set of criteria and process to define foreign adversary with a focus on entities or persons and not entire countries. This approach would allow for identification of foreign adversaries in a specific and measurable way that provides notice to entities engaged in ICTS transactions and is thus susceptible to counterparty screening and other proactive compliance measures.

[6] Proposed Rule § 7.101.

Sufficiently clear and settled authorities under U.S. law may not currently exist such that the Secretary is able to lawfully and consistently designate foreign adversaries at this time, in alignment with other similar authorities. For instance, the Federal Acquisition Security Council (FASC) is currently examining existing legal authorities as it considers how to implement the SECURE Technology Act's provisions regarding excluding and/or removing foreign suppliers from USG procurements, a process which will obviously require the identification of adversarial companies who pose an unacceptable level of security risk. The FASC is still evaluating how to implement those provisions in light of current authorities and is expected to issue an interim final rule for comment within the next few months, followed by a final rule by the end of 2020.

The lack of settled, clear authority regarding how and whether the Secretary should go about designating foreign adversaries, coupled with the fact that designating one or more foreign adversaries is clearly necessary before the Secretary may establish the required nexus to a foreign adversary to block, prohibit or unwind any ICTS transaction, suggests that, at a minimum, Commerce should delay issuing any final implementing rules until any legal or process uncertainties regarding the SECURE Technologies Act or other authorities are clarified, in order to develop a consistent process for designating individual companies as foreign adversaries.

B. Avoid Duplicative Review Processes

In order to make this authority as targeted as possible, Commerce should consider existing mechanisms already in place for reviewing transactions potentially raising national security risks, including the Export Administration Regulations (EAR), International Traffic in Arms Regulations (ITAR), CFIUS, relevant provisions of the John S. McCain National Defense Authorization Act for FY 2019 (including Section 889, FIRRMA, and ECRA), relevant provisions of the SECURE Technologies Act; the recent FCC restriction on certain telecommunications equipment in U.S. 5G networks, and Team Telecom processes with an eye toward deconflicting the types of transactions subject to review by each of these regimes. This would ensure that a single transaction is not caught up in multiple review processes.

In particular, ITI recommends that Commerce include a limiting principle for the use of this authority, similar to CFIUS: if other legal authorities exist to mitigate and/or address an identified national security risk, this rule should not apply. For example, CFIUS operates under a statutory and regulatory rule that its authorities apply only when the government's national security concerns are not adequately addressed through other laws and regulations.[7] We recommend that a SNPRM clarify that any transaction that has undergone

[7] *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

or is under review via another process will not be subject to subsequent or parallel review under a SNPRM. Given the overlap of U.S. government agency national security assessments, a clearance of a specific transaction under one U.S. federal regime should preclude the review of that same transaction through another national security review process (e.g., outbound transactions should not be covered by this rule as they are already regulated by existing export control regimes such as the Export Administration Regulations and International Traffic in Arms Regulation.)

C. Evaluation Criteria Should Be Country-Agnostic

The EO provides that Commerce can designate either countries or companies as "foreign adversaries." ITI strongly recommends that as these rules are further honed, Commerce ensure that any resultant narrowing is country-agnostic, an approach which seems better aligned to the fact-specific case-by-case approach contemplated by the NPRM. We do not support the naming of entire countries as foreign adversaries, nor would we advocate for categorical exclusions or inclusions on solely the basis of country of origin. The legal basis for such overbroad designations is unclear and would likely capture many entities who in fact pose no appreciable risks to national security or critical infrastructure security, and might actually exempt entities from review who could pose such risks.

D. Narrow Scope to Address National Security Objectives

We encourage Commerce to narrow the scope of the NPRM to provide businesses with a greater level of certainty about what sorts of transactions will trigger a review based on those transactions that present national security risks. As drafted, even routine commercial transactions will be covered by this rule.

While it is difficult for industry to meaningfully identify and suggest categorical exclusions without more information about the specific threats and vulnerabilities that would be the target of these regulations, Commerce should at a minimum categorically exclude transactions that lack a nexus to a specific threat or vulnerability articulated in U.S. government intelligence or vulnerability assessments. If a transaction does not implicate a specific, identified threat or vulnerability, it should not be covered by the rule.

It might also be helpful to develop a list of mitigating and aggravating factors, which may help Commerce identify whether a particular transaction is more or less likely to present a risk to national security, or to the security of critical infrastructure. Examples of categories that may be inherently low risk and thus should be considered as candidates for exclusion include: (1) mass market electronic devices primarily intended for home or small office use; or (2) commercial off-the-shelf (COTS) items that do not require modification or

---

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

maintenance over their lifecycle. Although the tight timeframe for responding to the NPRM has made it challenging to fully develop and vet a full list of ICTS categories that are unlikely to create such security risks, ITI stands ready to work with Commerce and other USG and industry stakeholders to further analyze ICTS and develop a list of categories that may be ripe for exclusion.

Commerce should also look to adopt the same exclusions as those outlined in Section 889: (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.

An EAR-like approach might also be useful in this context and would provide companies with more granular notice as to what types of transactions might be in scope. In particular, Commerce could consider co-opting the Export Control Classification Numbers (ECCN) classification system, which would allow for concerning technologies to be clearly identified where appropriate.

We believe such a targeted approach coupled with other sources of relevant information would be more consistent with the overarching, case-by-case fact-specific and risk-based approach that Commerce is seeking to take to the NPRM.

E. Establish a Pre-Clearance Method and Waiver Process

The breadth of the NPRM would create significant business and competitive risk and uncertainty for U.S. companies seeking to comply with the rule. This uncertainty will have the unintended consequence of technology companies' U.S. operations pressing the Department for pre-clearances or pre-approvals for nearly every transaction with foreign partners. Staffing and funding a pre-clearance process would be costly for both U.S. companies and for the Department and may hinder U.S. economic growth and U.S. company competitiveness. However, even though the rule as drafted would prompt an inordinate number of pre-clearance requests, foregoing any form of pre-clearance process entirely in favor of widespread uncertainty is an even worse result. The Department has the power to significantly reduce demand for pre-approvals by narrowing the scope of the NPRM and by defining safe harbors and excluded transaction categories.

Commerce should establish a formal or informal pre-clearance process focused on notification. Companies should have the option to notify a transaction to Commerce, with a reasonable period for Commerce to determine whether to pursue further evaluation or not. If the latter, companies could proceed with a safe harbor. In addition to providing more certainty to business, such a process would give the government more insight into the proposed transaction while also ensuring that the parties to the transaction understand what national security bounding conditions will apply in a given set of circumstances.

ITI also recommends that in redrafting this rule as an SNPRM, Commerce set up a "waiver process," similar to that laid out in Section 889. Impacted entities can work with the U.S.

government to develop a mitigation plan to resolve issues identified through the disclosure process, instead of being forced to completely unwind a transaction. It is our view that Commerce should be required to pursue the least restrictive option in each situation, looking first to mitigation and only to prohibition or unwinding as a last resort and even then, only after it has been made clear that no other legal authorities are in place to address the concrete, identified national security risk.

F. Issue Advisory Opinions

The NPRM states the Secretary will not issue advisory opinions or declaratory rulings with respect to any particular transaction. ITI recommends that Commerce instead allow for advisory opinions to be issued. This would provide concrete guidance to businesses seeking to comply with the EO. ITI would be open to discussing with Commerce the format that such an advisory opinion process might take.

5. Questions Posed in the NPRM

- *Are there instances where the Secretary should consider categorical exclusions? Are there particular classes of persons whose use of ICTS can never violate the EO?*

ITI recommends that transactions that were completed prior to May 15, 2019 be excluded from review.

Any transaction that does not demonstrate a direct nexus to a foreign adversary or national security risk, or that is covered by another regime with national security oversight, should be excluded from review.

Transactions involving personal services, such as those provided by engineers, should be excluded from review.

Additional suggestions regarding potential mitigating or aggravating factors, and examples of such factors, are listed above in section 4d.

- *Are there transactions in which risks could be reasonably mitigated? What form could such mitigation measures take?*

There are multiple ways in which risks inhering in transactions can be reasonably mitigated and such technical mitigations should be discussed with industry subject matter experts after Commerce issues a detailed SNPRM. Industry is constantly innovating to address the dynamic threat environment and those innovations that support risk management efforts can and should be taken into account when assessing the effect of a transaction.

ITI recommends that Commerce explore how and in what circumstances a company's adherence to certain risk-management standards or principles should be considered as mitigating factors in this regard. 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.[8]

- *If mitigation measures are adopted, how would the Secretary be informed that parties are actually taking mitigation measures? How would he be kept informed of any changes in circumstance that could either make mitigation obsolete or alternatively, allow for adequate mitigation?*

It is difficult to answer this question without additional specificity regarding the threats and vulnerabilities that Commerce is seeking to address. Where appropriate, we recommend that Commerce rely on existing authorities to mitigate and/or manage risk.

We suggest that any audit processes to monitor mitigation and affirmative relief processes should be defined to provide for effective oversight on both continuing compliance and relief when continuing compliance is no longer needed. This could be modeled on the CFIUS process.

- *How should "dealing in" or "use of" be interpreted?*

We suggest an approach to interpreting these terms beginning on p. 4 of our comments. We suggest completely eliminating terms used to describe a "transaction" that are redundant – such as "dealing in" -- and to clearly articulate what commercial activities are not intended to be captured (e.g., export transactions covered by EAR).

- *Should additional recordkeeping requirements be mandated?*

No additional recordkeeping requirements should be mandated. Companies should be expected only to keep records as they do in the normal course of business.

6. Conclusion

ITI appreciates the opportunity to submit comments in response to the NPRM. As stated at the outset, we believe industry and government must work together to achieve the trusted, secure, and reliable global supply chain that is a necessary priority for protecting national security and an indispensable building block for supporting innovation and economic growth. Working together to develop a narrowly tailored and focused rule will help to achieve the shared objective of strengthening our collective security without harming U.S. technological leadership and competitiveness.

The outcome of this rulemaking process is critical to all ITI member companies and as such, as a next step we strongly recommend that Commerce issue refinements to this rule in a SNPRM, including a comment period longer than thirty days, to allow for maximum stakeholder engagement and input. We look forward to working with the Commerce Department on revising the framework laid out in the rule in a manner that results in a

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

systematic, focused and calibrated approach that will effectively achieve the national security objectives laid out in the underlying EO. Please continue to consider ITI as a resource on this issue going forward, and do not hesitate to contact us with any questions regarding this submission.

Sincerely,

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