Coalition of Services Industries
Written Comments

Proposed Rule
on Securing the Information and Communications Technology and Services Supply Chain

Department of Commerce
DOC-2019-0005
January 10, 2020

The Coalition of Services Industries appreciates the opportunity to provide comment on the proposed rule on "Securing the Information and Communications Technology and Services Supply Chain." CSI is the leading industry association devoted to promoting the international objectives of the U.S. services sector. Our members include companies that provide services both domestically and internationally, including information and communication technology services, financial services, express delivery and logistics, media and entertainment, distribution, and professional services.

CSI supports the U.S. government's efforts to pursue targeted and thoughtful national security scrutiny of the technology supply chain, yet our members are concerned that implementation of the rule as drafted would have a negative impact on global services trade. The proposed measure would subject an unnecessarily broad scope of ICT transactions to administrative review and potential reversal. Moreover, the lack of guidance as to which transactions would be acceptable and the potential for the review and reversal of contracts would create a troubling degree of uncertainty for services firms.

The rule could also create a potentially harmful global precedent if other countries opted to mirror the U.S. approach as currently outlined. A proliferation of such measures would have a chilling effect on international commerce, with governments around the world erecting barriers to technology services and hardware imports – including those from the U.S.

With the goal of achieving national security objectives while increasing certainty for businesses and avoiding major disruptions to the global services economy, we have outlined below recommendations intended to provide greater clarity on the reach and scope of the proposed rule and key elements of the review process.

***

Pursue risk-based and transparent approach to ensure scope is narrowly tailored to national security concerns. We believe that whenever the International Emergency Economic Powers Act (IEEPA) is invoked to justify an administrative action on the basis of national security, it is critically important that

the proposed measures not be overbroad and be narrowly tailored, transparent and clear in addressing specific national security concerns.

In this case, the underlying supply chain executive order was promulgated to respond to risks posed by transactions with specific ICTS suppliers deemed worthy of national security scrutiny, most notably certain telecommunications equipment suppliers. Yet the resulting rule would extend government regulatory powers over a far broader universe of common commercial transactions. Once-routine transactions involving common ICTS could become subject to possibly lengthy government vetting – an outcome that would hurt U.S. business productivity without yielding commensurate national security benefits.

For example, the use of the term "digital economy" could implicate a very wide universe of goods and services, including many consumer-facing and business-to-business applications with no clear nexus to national security. Because most U.S. services firms rely on ICTS for core business functions, such as communications, marketing, distribution and delivery, the proposed rule could have a disruptive effect on routine operations across many services industries.

To ensure the proposed rule achieves the desired result while minimizing disruptions to business, we urge the administration to employ a risk-based approach, in line with long-standing federal government practice, which would narrowly focus its review to goods and services with a clear nexus to national security. Such an approach should be transparent and set out specific criteria for identifying foreign adversaries and evaluating transactions.

We also recommend establishing a standard of "reasonable care," under which companies that follow best practice standards for due diligence and careful evaluation of goods and services are acknowledged to have acted in good faith and would therefore not be penalized for transactions that could reasonably be judged not to fall within the scope of the law. The Customs and Border Protection and Internal Revenue Service agencies have similar standards.

In addition, to provide greater transparency as to the types of technology most likely to attract government scrutiny, it would be helpful for the Commerce Department to publish an annual public report with summary information on the number of transactions reviewed, blocked, and mitigated, as well as the category of ICT goods and services involved and national security rationale for the government's actions. Names of parties to the transactions should not be included.

Limit scope of ICTS under potential consideration. The rule offers no parameters to limit the scope of equipment and services in question to those products that present national security risks. Rather, the rule includes even routine commercial transactions regardless of risk. The scope is overly broad, which will undermine compliance efforts. While difficult to suggest categorical exclusions without more information about the specific threats and vulnerabilities that would be the target of the rule, specific categorical exclusions could include, but are not limited to:

- mass market electronic devices primarily intended for home or small office use;
- commercial off-the-shelf (COTS) items that do not require modification or maintenance over their lifecycle;

- items that are or can be effectively mitigated, such as through encryption;

- Local Area Network (LAN) equipment including routers, switches, network interface cards, and networking cables;

- software, including entertainment software such as video games, systems software and applications software such as operating systems, security software, file management systems, data processing applications, and other software applications designed for commercial use;

- products and transactions that are both subject to and permissible under other national security laws and regulations (e.g., CFIUS, ECRA, Team Telecom (FCC)

- Outbound versus inbound transactions, particularly as these are already regulated by existing export control regimes such as the Export Administration Regulations and International Traffic in Arms Regulations; and

- transactions involving categories of products that are non-sensitive or non-threatening items such as EAR99 item

- On a related note, Section 889 of the NDAA provides for security reviews of telecommunications equipment and services but allows exceptions for telecom service that connects to the facilities of a third-party (such as backhaul or roaming) and "dumb" telecom equipment that cannot route user traffic. In the interests of consistency, we would recommend that the proposed supply chain rule incorporate the same exemptions.

In addition, Commerce should establish a clear process and standards for evaluating 1) whether a transaction is within the scope of the EO; and 2) if it is covered by the EO, whether it poses a risk to national security. In particular, Commerce should clarify that the mere funding of a network deployment or the mere presence of equipment or technology developed or distributed by a designated entity are not sufficient to create national security concerns. We also recommend that that if sufficient controls and/or mitigation can be demonstrated to prevent a material risk to national security, that it be exempted.

Define or clarify key terms. Certainty in the application of the rule is critical for all interested parties. Definitions should be revised to provide the certainty required for continuity of business, future transactions, compliance and enforcement, including at a minimum:

- Developing and applying transparent, narrowly-tailored criteria for what would constitute a foreign adversary before evaluating any transactions. This determination should focus on specific individuals or entities rather than whole countries. Such revisions are necessary to: (1) create certainty for U.S. companies when entering into ICTS transactions and; (2) alert industry to foreign adversaries of concern so that industry can evaluate and mitigate risks in advance through compliance efforts.

- The definition of "transaction" is overly broad and unclear. The current definition is as follows: "The transaction involves any property in which any foreign country or a national thereof has an interest (including through an interest in a contract for the provision of the technology or service)." This reference to "contracts" may be read expansively to include commercial agreements in which there is no direct nexus to public telecommunications networks within the United States, such as the

following: the lease of network infrastructure capacity outside the United States; the termination or carriage of international data traffic entirely outside the United States; and/or technical arrangements necessary to effectuate international roaming of various types (e.g., voice, data, messaging) and transiting through the United States without interconnecting with any public U.S. networks. Requiring review of all such routine agreements could be unduly burdensome and is not directly related to the EO objective.

The proposed rule should make clear that information technology communications-related projects entirely outside the United States are outside the scope of the potential prohibitions, even if a U.S. person is involved in a commercial aspect (for example, financing or owning a stake in the non-U.S. joint venture involved in the project).

Accordingly, we recommend narrowly tailoring the scope of the proposal to exclude transactions in which the services or technology in question are outside of the United States.

- We recommend that the rule be further clarified as only covering inbound transactions.

- The definition of the term "transaction" should also be revised to remove "dealing in" and "use of." This characterization is too broad and there is no way to know whether stakeholders will be captured merely for using or "dealing in" an item.

- The definition of "interest" should be clearly defined to include only a current interest that affords the foreign party actual physical control or access to ICTS.

- Only the interest of a foreign adversary should be considered, and that interest should only be present where the ICTS transaction directly involves a designated "foreign adversary." Interest of a "foreign country or a national thereof" is irrelevant to the determination and Section 7.101(a)(2) should be struck.

- Also, 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." 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 that the intent is to capture majority or controlling interests.

- Commerce should not determine that a party is owned or controlled by a foreign adversary where a foreign adversary does not have a controlling interest in voting shares or the ability to appoint a majority of the board. Further, Commerce should exclude transactions involving companies "owned or controlled by" foreign adversaries when they are headquartered in an allied nation or all production of ICT occurs in an allied nation.

- As drafted, the rule does not provide clarity on the criteria that will be evaluated in determining whether a transaction poses an "undue risk" or an "unacceptable risk." To avoid confusion, the rule should only use "unacceptable risk" as this would seem the most fitting for national security-related concerns.

Limit jurisdictional reach. The text of the rule says it would apply to both people and property subject to U.S. jurisdiction. This classification could conceivably extend to wholly foreign activities conducted by

foreign subsidiaries of U.S. companies as well as property—goods or services –that are not acquired or used in the United States.

If the rule is interpreted to apply to foreign corporate offices as well as those on U.S. territory, its sheer breadth would unreasonably burden U.S. services firms with an impossible compliance task and make it unlikely to achieve meaningful implementation. It would be exceedingly difficult for the Commerce Department to adequately scrutinize any "acquisition, importation, transfer, installation, dealing in, or use" of ICT goods and services both in the U.S. and in the vast network of overseas offices operated by American companies.

Further, such an overly broad interpretation could create an extreme burden for the department, which might conceivably be required to review every transaction relating to ICTS of U.S. foreign subsidiaries in foreign markets, including routine operations such as local internet and telecommunications and marketing services. The compliance burden and related uncertainty would put U.S. companies operating in overseas market at a competitive disadvantage vis-à-vis foreign competitors.

The proposed rule should be narrowed to make clear that it does not apply to transactions involving products or services used outside the United States.

Similarly, Commerce should strike the reference to persons "subject to the jurisdiction or direction of" a foreign adversary. This definition could apply to any person located in a foreign country where a government is deemed a foreign adversary, regardless of citizenship.

Remove retroactive provisions that create tremendous uncertainty. The proposed rule would introduce a very substantial degree of uncertainty by raising the prospect that completed transactions could be reversed by the government. The absence of any effective statute of limitations, coupled with Commerce's refusal to allow for advisory opinions, means that any such unwinding could take place months or even years after the fact. Accordingly, the proposed rule should focus instead on pending and future transactions, provide for issuance of advisory opinions, and allow for parties to voluntarily notify the transaction with safe harbor if Commerce does not pursue evaluation within a reasonable timeframe.

Create optional clearance process and delineate timelines. The Federal Register notice does not stipulate whether companies will have the option to notify Commerce or which types of digital transactions they must disclose. It also does not specify at what point in contract negotiations such a notification should be made. We recommend that the rule allow for a voluntary process under which companies have the option to submit notification of a transaction to the government. There should then be a reasonable period for Commerce to undertake an inquiry, after it has been provided notice of an intended deal by one or both parties. Should Commerce elect not to pursue an evaluation following a voluntary notification, there should be safe harbor for the transaction going forward.

Where a review is commenced for whatever reason, the rule as drafted does not include a deadline by which Commerce must make its preliminary determination. During that indeterminate period, we recommend the agency clarify that companies would be allowed to undertake other transactions. If a firm were forced to put other important transactions on hold for the duration of a review, it may suffer serious competitive consequences.

We would also urge the department to consider adopting a minimum of 60 days for the post-notification response period and review process, instead of the current 30 allotted days.

Then, barring any objection by the Commerce Secretary in the form of a preliminary finding (as described in the proposed rule), the presumption should shift to there being no unacceptable risk.

Once that window closes, the Commerce would not be foreclosed from exercising its authority. However, the standard of proof should be elevated – for example, to clear and convincing evidence of the requisite harms.

Minimize potential for abuse of "private party" request for review. The triggering factors for review as proposed in the rule also raise yellow flags. Under the approach described, which allow a "credible" private party to request an evaluation, a company would have a malign incentive to propose the review of a competitor. A firm could handicap a business rival simply by initiating what may be a prolonged and distracting government review process. We recommend that the department delete the provision expressly stipulating that an evaluation can be triggered by information from private parties.

If Commerce does maintain that a private party's submission of information may trigger the review of a transaction, we strongly urge the department to share that information with the entity subject to the review. It is only fair that a company be provided with the opportunity to respond to what may be misleading or false claims from a rival party.

Promote greater interagency review. Another concern is what appears to be a relatively limited degree of interagency consultation and oversight throughout the review process. In contrast, in administrative processes such as CFIUS, a substantial degree of interagency review serves to maintain systemic checks and balances during the process.

To help ensure a deeper level of interagency discussion, we recommend instituting a process in which the agency leads cited in the proposal convene a meeting or conduct a vote on whether a given transaction should be subject to the rule, whether it poses a risk to national security, and appropriate enforcement measures.

The rule at present allows the Commerce Secretary to delegate decision-making authority to a "designee." We recommend that the delegation only be permissible to Senate-confirmed appointees. It is appropriate to reserve decision-making powers for a senior appointee so that Congress can hold the executive branch accountable, including by holding hearings and submitting requests for information to personnel subject to Senate confirmation.

We are particularly concerned by a provision that allows the Commerce Secretary to declare an emergency that would eliminate any need for further interagency discussion. Under the proposed rule, the Secretary could then "dispense with any or all of the procedures" set forth in the rule and grant his or her own agency decision-making power unchecked by any other government constituents. We believe such a grant of authority to be excessive, disproportionate to the goal of improving supply chain security, and inappropriate for a peacetime economy.

Align and ensure consistency with existing regulatory regimes. There is a risk that the process under consideration may overlap with existing administrative regimes including CFIUS, Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 ("Section 889"), Team Telecom, and

the recent FCC restriction on certain telecommunication equipment in U.S. 5G networks. At present, it is not clear whether the supply chain review would take place in addition to or in lieu of these other processes. Layering on yet another review process, with its own distinct rules, personnel, and timeline, will exact additional costs in both money and time. The cumulative toll of the aforementioned requirements will be significant.

For this reason, we suggest the government provide that transactions that have undergone one of the reviews noted above would be exempt from subsequent supply chain reviews, except under truly unusual and compelling circumstances. A clearance by one process should either preclude or at least streamline review by another national security process.

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. When the Department identifies a material risk, the Department 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).

We also encourage the Department to modify the language in the final rule to clarify that a common carrier will not 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 providing transportation services to one or more of the parties to a transaction that has been prohibited in a final written determination made by the Department or permitted subject to mitigation measures. Even if summaries of the Department's final determinations will be made public, common carriers cannot be expected to know whether a particular shipment is part of a transaction that has been prohibited or restricted by the Department. Payment networks should equally be excluded from liability for providing electronic payment services to such parties because they cannot be expected to know about the specific activity underlying the payment. Therefore, common carriers and payment networks should not face liability under this regulation unless it can be demonstrated that the entity had actual knowledge that a particular shipment or payment transaction was prohibited.

Protect against disclosure of sensitive information. The Commerce Department has said it will issue public reports detailing its final determinations. But while it has pledged to maintain the confidentiality of business information, it is conceivable that releasing even basic information, such as the names of suppliers or place of manufacture, could inadvertently implicate specific companies.

In order to fully participate in the review and potential mitigation process, businesses will need to be assured that any sensitive information will be protected. The final rule should clearly describe procedures to protect business confidential information that is submitted to the department by parties that are subject to reviews, such as ensuring that that the U.S. government will not release related information in response to Freedom of Information Act requests.

Establish appeals process. One of the most concerning aspects of the rule is that the government could force the reversal of a transaction that a company entered into in good faith and in the absence of any government advice to the contrary.

To recap, the rule sets forth a scenario in which a company could undertake a transaction involving digital hardware or services in good faith, with no reason to suspect it might fall subject to government

scrutiny. The company could then learn that a review of that transaction was underway, the duration of which would be unclear. In the end, after a potentially lengthy period, the government could end up forcing the company to exit its contract or reverse an acquisition. The entirety of the process, which would likely require significant investments in corporate time and resources, could cause significant disruptions to business operations – all because the company did not adequately understand which technologies or transactions would fall within the scope of the supply chain review.

While we would hope such situations would be rare, the rule as proposed could very well result in such scenarios. The supply chain measure is so broadly scoped, and there are so many questions about how it would work in practice, that one can well imagine situations in which companies with the best of intentions might unwittingly run afoul of it. In light of these uncertainties we believe it is essential to incorporate an appeals process into the procedure, thus providing an additional layer of due process and protection for those subject to the review.

Assume other countries will emulate U.S. approach. While the Commerce Department has framed its proposal in terms of improving U.S. domestic security, it will likely have international repercussions. There is a high probability that other countries, which have also begun considering issues of supply chain security, may copy aspects of the American approach.

It is certainly possible that more governments, following the U.S. example, might opt to impose bans on foreign products in the name of national security and without providing a clear explanation. Thus, it is all the more important that the U.S. implement its own supply chain review with the greatest possible degree of clarity and attention to due process.

Conclusion. The Federal Register notice for this proposal cited the government's desire to avoid "inadvertently preclud[ing] innovation or access to technology in the United States." Unfortunately, CSI members believe that the regulation as drafted could risk undermining innovation and access to technology.

The goal should be to develop a proposal implementing the supply chain executive order that provides a transparent process with a clear set of definitions and guidelines and is grounded in a risk-based approach. As such, we urge the government to substantially revise and narrow the current proposal based on further interagency consultation as well as stakeholder input.

In addition, given the important implications of the supply chain rule for the health of the U.S. services economy as well as broader global trade, we strongly encourage the government to provide a second stakeholder comment period before finalizing the measure. Thank you for the opportunity to provide comments.