SEMICONDUCTOR INDUSTRY ASSOCIATION

Uploaded via http://www.regulations.gov at docket number DOC–2019–0005
Sent via email to ICTsupplychain@doc.gov

January 10, 2020

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

Re: Comments of Semiconductor Industry Association to Proposed Rule Entitled "Securing Information and Communications Technology and Services Supply Chain," 84 Fed. Reg. 65316 (November 27, 2019)

Ref: Docket No. 191119-0084; RIN 0605-AA51

Dear Mr. Young:

The Semiconductor Industry Association (SIA) is the voice of the U.S. semiconductor industry, one of America's top export industries and a key driver of America's economic strength, national security, and global competitiveness. Semiconductors – microchips that control all modern electronics – enable the systems and products we use to work, communicate, travel, entertain, harness energy, treat illness, and make new scientific discoveries. The semiconductor industry directly employs nearly a quarter of a million people in the United States, and is the nation's 4th largest export by revenue. In 2018, U.S. semiconductor company sales totaled $209 billion, and semiconductors make the global trillion dollar electronics industry possible. SIA seeks to strengthen U.S. leadership of semiconductor manufacturing, design, and research by working with Congress, the Administration and other key industry stakeholders to encourage policies and regulations that fuel innovation, propel business and drive international competition.

It is well established that the ICTS industry thrives on a complex, global supply chain created out of necessity and market need. Although the trade activity of the semiconductor industry in the United States is primarily focused on exports, the economic success of our members and their customers is dependent on a variety of global activities. Most of these activities would fall within what the Proposed Rule defines as a "transaction[s]," *i.e.,* "the acquisition, importation, transfer, installation, dealing, in and use of items and services" in the Information and Communications Technology and Services (ICTS) Supply Chain ("ICTS Supply Chain"). Because such transactions almost always involve ICTS items and activities in international trade, the Proposed Rule, if implemented, would subject to its jurisdiction essentially all economic activity of our member companies. Thus, we are pleased to provide these comments in support of the

national security objectives at issue and on how those objectives can be accomplished more effectively and without unnecessarily harming the U.S. semiconductor industry.

Section I contains general comments and our request for a supplemental notice of proposed rulemaking that is more tailored to addressing the threat at issue. **Section II** contains our responses to the specific questions posed in the notice. **Section III** contains additional comments and suggestions on other aspects of the Proposed Rule.

I. General Comment and Request

Commerce should work with its interagency partners to develop and then publish a supplemental advanced notice of proposed rulemaking – *i.e.*, a second proposed rule – that takes a risk and threat-based approach to addressing specific, identified threats to the ICTS Supply Chain. To accomplish this objective, the second proposed rule should (i) identify more specifically the types of transactions that would be covered by the rule; (ii) identify the specific criteria that the Department will apply to identify entities of concern; (iii) describe the specific equipment, technology and services of concern; and (iv) contain an licensing or other safe harbor process to give parties confidence that covered transactions will not be unwound or altered after completion.

SIA opposes the implementation of the Proposed Rule as written because it is a standard-less delegation of broad "case-by-case" authority over economic activity that would impose a cloud over domestic transactions and most international trade transactions related to technology. For example, a U.S. or foreign person would not be in a position to know which types of transactions involving non-U.S. parties could lead to a unilateral decision by the Secretary of Commerce to block, alter, or order the unwinding of a transaction days, weeks, months, or years after its completion.

Our concerns with the proposal also include the following:

- The Proposed Rule is not tailored to address specific threats by specific entities and would have broad jurisdiction over activities involving ICTS items that are "designed, developed, manufactured, or supplied by" persons "owned by, controlled by, or subject to the jurisdiction of a foreign adversary." In practice, these roles could be a person, company, or country known only to the Secretary. (§§ 7.101(a)(4) and 7.2) Should Commerce identify specific *countries* as foreign adversaries, local ICTS purchases within the boundaries of a "foreign adversary" by a wholly owned affiliate of a U.S. company are at risk because the affiliate would be "subject to the jurisdiction of a foreign adversary."

- The rule would apply to "*any* hardware, software, or other product or service primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means, including through transmission, storage, or display." (§7.2). As applied, the provision covers virtually every electronic

item containing a semiconductor that exists, including everyday consumer items such as cell phones and laptops.

- The rule would have jurisdiction over "*any* acquisition, importation, transfer, installation, *dealing in, or use of any*" ICTS items. In other words, merely using a consumer electronic device would fall within the covered activities. (§ 7.2) Importing electronic components from a wholly owned foreign subsidiary for manufacturing in the United States would be covered. Activities by a foreign bank in providing financing for such imports would also be covered. There are many other such examples that certainly go way beyond the types of transactions warranting control to address the threats at issue.

- The rule, as proposed, would give the Secretary unfettered authority to alter, block, or unwind otherwise completely legal, uncontrolled commercial transactions – even if cleared by CFIUS or other authority – if he or she believes, in his or her sole discretion, the transaction "poses an unacceptable risk to the national security of the United States . . . ." The rule moreover provides no practical insight into the standards or criteria relevant to the Secretary's exercise of such discretion. That is, it does not contain enumerated national security factors – beyond the broadly scoped, general principles stated in §7.101(a)(5)(i)–(iii) – that the Secretary would consider when making determinations, or that a court could analyze to determine if the rule was properly applied.

- The rule would allow a jurisdictional determination to include, but not be limited to, considerations of the "laws and practices of the foreign adversary; equity interest, access rights, seats on a board of directors or other governing body, contractual arrangements, voting rights, and control over design plans, operations, hiring decisions, or business plan development." This broad grant of authority could apply to almost any company from any country. (§7.101(b))

- The rule casts deep uncertainty over the status of global business relationships. To remedy this, Commerce should, among other things, set forth the criteria for identifying entities of concern. The criteria should be consistent with, and not duplicate, current authorities. Clearer criteria in this regard will provide sorely needed guidance to industry when engaging in transactions in our global supply chain.

- The rule would give the Secretary the complete discretion to dispense with any of the foregoing broad and limited procedures if, in his or her sole opinion, and without any other process, oversight, or interagency review and clearance, public harm is likely to occur or the national security interests require it. (§7.104)

SIA believes such a broad jurisdictional reach, without meaningful criteria on when or how it will be applied, is more harmful than helpful because successful international trade and ICTS transactions depend upon certainty and clarity. If Commerce implements the Proposed Rule as

drafted, it will inject significant *un*certainty into international trade and domestic transactions. Such uncertainty will make foreign persons less willing to do business with U.S. companies.

The result will be direct economic harm to the U.S. ICTS and related industries, which undermines our overall national security. As noted by many sources, overbroad policy responses to legitimate issues stifle innovation, hinder technological leadership, and harm the competitiveness of U.S. industry. We therefore support laws, regulations and policies that address identifiable national security risks while imposing the least possible burden on U.S. commerce. With greater interagency collaboration, industry participation, and an SNPRM tied to the threat and vulnerability assessments at issue, we believe that such an objective is achievable.

II. Reponses to Specific Questions Posed in the Notice

The following are our responses to the specific questions Commerce posed in the notice.

Question 1: *Are there instances where the Secretary should consider categorical exclusions? Are there classes of persons whose use of ICTS can never violate the Executive Order? If so, please provide a detailed explanation of why the commenter believes a particular transaction can never meet the requirements of the Executive order.*

Response 1: Yes. At a minimum, Commerce should categorically exclude transactions that lack a nexus to a specific threat or vulnerability articulated in ODNI or DHS's threat and vulnerability assessments. If a transaction does not implicate a specific, identified threat or vulnerability, it should not be covered by the rule implementing the Executive Order (EO). Such an approach would add significant clarity to the scope of the rule without materially affecting the government's ability to address the general risks articulated in the Executive Order, particularly in light of the periodic and annual threat and vulnerability updates called for in the Executive Order.

In addition, absent a specific risk, Commerce should exclude consideration of transactions that involve ICTS manufactured by an entity that is merely "subject to the jurisdiction" of a "foreign adversary." This could subject entire classes of products made in specific countries to a prohibition, regardless of the technical characteristics of the product or the parties involved in the transaction. This approach appears to be inconsistent with recent U.S. government statements about its intent to further integrate key global ICTS trading partners (*e.g.*, Politico, *Trade rep: China will determine success of trade deal* (Dec. 15, 2019)).

Furthermore, the rule should exclude transactions subject to and permitted under other relevant national security regimes such as CFIUS, export controls,

economic sanctions regimes, authorities overseen by the Federal Acquisition Security Council (41 U.S.C. § 1323), authorities overseen by U.S. Customs and Border Protection, including the Minimum Security Criteria and Guidelines for the Customs Trade Partnership Against Terrorism (CTPAT), authorities overseen by the Federal Communications Commission (FCC), authorities overseen by the Federal Energy Regulatory Commission (FERC), Sections 881 and 889 of the National Defense Authorization Act for 2019 (among others), Defense Federal Acquisition Regulation Supplement (DFARS) subpart 239.73, DoD's "Do Not Buy" List or any DHS Binding Operational Directive (BOD) (among other federal policies), and other national security and supply chain authorities that address the same or similar risks as those outlined in the Executive Order. For example, the final rule should not grant the Secretary of Commerce authority to block, alter or undo a transaction already cleared by CFIUS or Team Telecom.

The rule should also exclude transactions "conducted by any person subject to the jurisdiction of the United States" where the connection to the United States is attenuated or divorced from the policy rationale underlying the Executive Order. Along those lines, transactions should only be considered "conducted by" a person subject to U.S. jurisdiction if one of the principal parties in the transaction (*e.g.*, the purchaser or the end-user) is a person or entity subject to U.S. jurisdiction. The mere involvement of a U.S. person, such as an employee supporting an international transaction, should not be sufficient to support review of a transaction by Commerce. Additionally, the second proposed rule should create a presumption against reviewing transactions where the foreign interest is a subsidiary, including wholly owned affiliates, of a U.S. company.

Regarding existing, new or evolving standards or compliance regimes for supply chain security across the federal government, the Rule should identify specific standards and processes for which compliance with such measures would make transactions eligible for categorical or other types of exclusion. These types of exclusions will facilitate cross-government consistency in improving supply chain security. Examples may 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.

Industry and government continue to build upon this body of work in ways that may offer Commerce opportunities to add new compliance frameworks for supply chain trustworthiness and risk mitigations, including ATIS's 5G supply chain group, the O-RAN Alliance, and the Telecom Infra Project's OpenRAN project group.

Question 2: *Are there transactions involving types or classes of ICTS where the acquisition or use in the United States or by U.S. parties would fall within the terms of the Executive Order's prohibited transactions because the transaction could present an undue or unacceptable risk, but that risk could be reliably and adequately mitigated to prevent the undue or unacceptable risk? If the commenter believes the risks of a prohibited transaction can be mitigated, what form could such mitigation measures take?*

Response 2: As noted above, the rule should not regulate activities that are subject to and permissible under existing regulatory regimes that also focus on protecting national security. For example, existing regimes designed to enhance supply chain security include FIRRMA and ECRA, which recently expanded the jurisdiction of (i) CFIUS in terms of inbound investment and (ii) the U.S. Department of Commerce in relation to its export control program. Creating overlapping regulatory regimes would create confusion and unnecessary burdens for business.

Furthermore, the Proposed Rule should prioritize mitigation measures over the prohibition of a transaction. Mitigation measures often are effective to address national security threats while ensuring global technological competitiveness, as demonstrated by CFIUS' successful track record. Giving priority in the second proposed rule to mitigation measures, acknowledging that they often can be effective to address national security threats, could help blunt any unnecessary and unjustified negative impact on commercial activity.

Question 3: *Section 1(a) of the Executive Order and the definition of ''transaction'' that the proposed rule would implement refer to ''acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service.'' How are these terms, in particular ''dealing in'' and ''use of,'' best interpreted?*

Response 3: Commerce should define key terms in the rule (*e.g.*, "acquisition," "importation," "transfer," "installation") according to industry-accepted or dictionary definitions to ensure their consistent application to all parties. That, however, still will not address the fundamental issue with the rule that the mere "use" of an ICTS device, such as a cell phone or a laptop, could be regulated if it were part of a transaction with a person, company, or country the Secretary identified as within the scope of an order.

In a second proposed rule, Commerce should remove the terms "dealing in" and "use of" from the definition of "transaction" as these terms capture activities far beyond what industry considers typical ICTS transactions. In the alternative, at the very least, "dealing in" and "use of" should link narrowly to the specific

threats and vulnerabilities at the heart of the ODNI and DHS assessments, and not capture general use or dealing in ICTS items.

Question 4: *As discussed above, the Secretary expects persons engaged in transactions will maintain records of those transactions in the ordinary course of business. Should the Department require additional recordkeeping requirements for information related to transactions?*

Response 4: No. Commerce should not impose any additional recordkeeping requirements for information related to ICTS "transactions" as defined in the draft regulations. Commerce should follow the model of numerous other regulatory regimes by only requiring the retention of records created or maintained in the ordinary course of business.

III. Additional Specific Comments

SIA offers the additional comments below for consideration by the Secretary. However, SIA does not believe that addressing any one of these comments on its own would resolve the significant concerns noted with the Proposed Rule discussed in **Section I** above.

A. Establish a System for Parties to Obtain Safe Harbor Letters or Authorizations to Engage in International Trade Transactions so that They Know It Will Not be Undone or Altered Later

Even with a narrowed and targeted scope in a second proposed rule focused on specific threats and vulnerabilities, parties should be able to participate in a process for obtaining clearance of covered transactions. This process would involve obtaining a license, authorization, or some other form of safe harbor to engage in a proposed transaction with comfort that the Secretary will not later alter or unwind the transaction days, months, or years after the fact. Such authorization procedures are a normal part of similar regulatory structures, including the closely related CFIUS and export control systems, which Commerce should study for best practices as part of this effort.

On a related note, the notice does not identify the agency within Commerce with direct responsibility for implementing, administering, and enforcing the final rule. Commerce should include such information in a second proposed rule to permit a public assessment of whether the responsible agency will have sufficient resources and experience in administering and enforcing such a novel rule. Commerce should also identify in the second proposed rule whether it has the necessary appropriations from Congress to administer and implement any final rule.

Importantly, U.S. based business have an imperative to minimize business and regulatory risk related to their transactions. Under the current proposed rule, the volume of transactions covered is enormous because – as noted before- the Information and Communications

Technology and Services Supply Chain is both globally integrated and a major driver of US GDP growth. Given this, the U.S. Government's current staffing and capacity for assessing transactions and issuing safe harbor letters or authorizations may not be adequate.

B. Establish Checks and Balances on the Use of Emergency Powers and the Withholding of Notice on National Security Grounds

Consistent with other similar authorities, the second proposed rule should require briefing and explanation to congressional committees of jurisdiction either prior to or within a reasonable time following the use of emergency authorities. Commerce should also impose limits on the Secretary's discretion by requiring that he provide notice "when consistent with national security." These limits could include a requirement for interagency clearance before taking such action.

C. Publish Unclassified Versions of the Threat and Vulnerability Assessments

Commerce should publish unclassified versions of ODNI and DHS's threat and vulnerability assessments for public review to allow for a better understanding of the scope of this regulatory review. Giving the public an opportunity to review the threat assessments – with sensitive or classified information removed – will add more credibility and transparency to the process, the proposed rules, and the problem to be solved. Industry could also thereafter provide higher quality comments on how to address the actual threats and vulnerabilities with the least amount of harm to U.S. commerce.

D. Annual Reporting to Congress

To encourage accountability, Commerce should require an annual report to Congress detailing activities and actions taken under this authority. These reports could take a similar format to CFIUS annual reports.

E. Limit Length of Review Process

To give parties greater certainty in developing their business plans, Commerce should (i) draft into the second proposed rule a 60-day or other reasonable limit on the review process; and (ii) develop narrow guidelines so that it may only extend the 60-day review process under a specific set of circumstances. After 60 days, unless justifiably extended, the transaction should be immune from government interference under the EO.

F. Instead of a Blacklist of "Foreign Adversaries," Create a Threat-Based Risk Assessment Approach toward Specific Items and Parties of Concern

In lieu of blacklists or whitelists of persons, companies, or countries deemed to be foreign adversaries (or not), the second proposed rule should adopt a risk-based approach toward particular types of transactions, not entities. For example, an entity involved in a risky

transaction today may undertake a completely innocuous transaction tomorrow under slightly different facts. Thus, the second proposed rule should adopt a risk-based approach (based on clearly stated criteria) that would capture only the first transaction, but not the second, even though both transactions may involve the same foreign entity.

G. Create a Formal Interagency Review, Clearance, and Appeal Process

The CFIUS, export control, and other regulatory systems designed to monitor and mitigate national security risks have a formal interagency clearance and review process. This allows the government to factor in the important equities and expertise of the various agencies involved. Such systems also prevent abuse, politicization, self-dealing and mistakes by preventing unilateral action on complex cases initiated solely by one government official.

When there is an interagency dispute, formal procedures should exist for appeals and a process for resolving them consistent with pre-existing standards that all can review and abide by. For these reasons, we encourage the creation of such a process in the second proposed rule. Finally, given the almost unfettered discretion provided to the Secretary in the Proposed Rule, the implementation of such procedures would both prevent arbitrary decisions and remove any shadows of doubt about whether a specific decision was based on motives other than national security concerns.

H. Create Standards Regarding Information Submitted by Private Parties

The Proposed Rule contains almost no information about how private parties would submit information about an ICTS transaction that they believe creates a national security and economic securityrisk. There are also no standards for the evaluation of such information. In its current form, the Proposed Rule would thus encourage the submission of information by foreign and domestic competitors seeking economic advantages, which, without any standards of proof, could lead to self-dealing.

The second proposed rule should contain clear evaluation standards and an articulable burden of proof for reliance on allegations by private parties or foreign governments, particularly with respect to economic information and information to a competitor's detriment. For example, the second proposed rule could limit Commerce's reliance on third-party information to that which it can independently corroborate. Also, if a third party's submission of information triggers a transaction review, the affected party should have the right to review and respond to what might be false information provided by a competitor or someone acting on behalf of a competitor.

I. Ensure Transparency of Notice and Reasoning

The Proposed Rule is ambiguous as to whether parties will always receive notice of a transaction review or will only receive such notice "as appropriate." The second proposed rule should require the Secretary to *always* provide direct notice to parties that their transaction is

under evaluation. While we appreciate that parties may submit an opposition demonstrating opportunities for mitigation, providing notice and ample time to parties to assemble that information is critically important to the review process and fundamentally fair.

J. No Retroactivity between May 2019 and the Effective Date

Consistent with other proposed rules issued under similar authorities and for similar national security purposes, Commerce should not extend the scope of the new regulatory regime to transactions undertaken since the May 15, 2019 effective date of the Executive Order. The application of retroactive authority over transactions completed since May could result in a taking without prior notice, particularly given the continued lack of clarity as to what transactions are subject to the Executive Order.

IV. Conclusion

SIA supports to the government's efforts to secure the ICTS Supply Chain in a manner that protects our national security while minimizing any *unnecessary* harms to U.S. commerce. Thus, our goal and request is to work with the Administration to craft, during a second round of public comments, a new rule that allows the government to fill the policy gap at issue without creating such significant uncertainty in the international trade marketplace involving ICTS items, particularly those involving semiconductors and related items.

We thus ask Commerce to publish, in a second proposed rule, a detailed, unclassified version of the threats that are not addressed by other areas of law – including those created by commercial semiconductors and related items. The second proposed rule should also provide at least 60 days for the public to work through what is clearly a difficult policy issue to regulate without unintentionally harming U.S. industry.

The semiconductor industry will continue to prioritize and invest in a safe and secure ICT supply chain. We appreciate the opportunity to provide these comments and we look for to working with the Department of Commerce on these shared goals.

Sincerely,

Maryam Cope
Director, Semiconductor Industry Association