Before the
DEPARTMENT OF COMMERCE
Washington, DC 20230

In the Matter of	)	
	)	
Securing the Information and Communications	)	RIN 0605-AA51
Technology and Services Supply Chain	)	Docket No. DOC-2019-0005

COMMENTS OF THE COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION

Dileep Srihari
Vice President and Senior Policy Counsel

Savannah Schaefer
Senior Director, Public Advocacy

COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION
322 4th Street NE
Washington, DC 20002

January 10, 2020

TABLE OF CONTENTS

Before the
DEPARTMENT OF COMMERCE
Washington, DC 20230

In the Matter of	)	
	)	
Securing the Information and Communications	)	RIN 0605-AA51
Technology and Services Supply Chain	)	Docket No. DOC-2019-0005

COMMENTS OF
THE COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION

The Computing Technology Industry Association ("CompTIA"),[1] the leading association for the global information technology ("IT") industry, respectfully submits these comments to the Department of Commerce ("Department") in response to the above-captioned Notice of Proposed Rulemaking ("NPRM").[2]

INTRODUCTION

CompTIA and our member companies encompass a wide cross-section of the IT sector, including software, technology services, telecommunications services, and device and infrastructure companies operating globally. Modern information and communications technology ("ICT") supply chains are inherently global and characterized by dynamic inputs that fluctuate to accommodate economies of scale. Our members are strongly committed to ensuring that the ICT products and services we offer and/or rely upon are based upon safe and secure supply chains.

[1] CompTIA supports policies that enable the information technology industry to thrive in the global marketplace. We work to promote investment and innovation, market access, robust cybersecurity solutions, commonsense privacy policies, streamlined procurement, and a skilled IT workforce. Visit www.comptia.org to learn more.

[2] 84 Fed. Reg. 65,316 (Nov. 27, 2019).

We also recognize that managing supply chain risk to the information and communications technology and services ("ICTS") ecosystem has important implications for national security. CompTIA and our members are committed to working constructively with the U.S. government – and indeed, have been doing so – to protect communications networks and other ICTS against identified risks. Executive Order 13873 ("EO")[3] has now tasked the Department with addressing the specific national security challenges identified therein while taking care to protect the competitiveness of U.S. companies. As the Department promulgates implementing rules, it has also been implicitly tasked with establishing sufficient due process and transparency safeguards, while also being mindful of actions taken by Congress and other agencies.

Unfortunately, the current Proposed Rule falls short of that threshold. As currently drafted, the Proposed Rule would represent a major government intervention into the U.S. economy with significant ramifications for U.S. companies' ability to compete in the global marketplace. In its current form, the Proposed Rule would subject every purchase, or even use, of ICT products or services in which any foreign company has an interest to the risk of unwinding upon the government's direction. This would be an extraordinary and unnecessary action.

We recommend that the Department begin the process of revising the Proposed Rule by defining more specifically the problem or problems to be solved. For example, Congress and other federal agencies have recently focused significant attention on these very same issues, but have limited any restrictions to federal government systems or the use of federal funding. As it

[3] Exec. Order 13,873, *Securing the Information and Communications Technology and Services Supply Chain*, 84 Fed. Reg. 22,689 (May 17, 2019) ("EO").

contemplates taking much stronger action here, the Department should closely examine the scope of its Proposed Rule and determine which transactions are truly necessary to fall within its scope. It should then narrowly tailor any rule – and a well-considered set of exemptions – accordingly, after first considering existing mechanisms and then differentiating appropriately among fact-driven, risk-based use cases. Narrow tailoring is particularly important given that U.S. actions in this space are likely to be a model followed by other countries, and there will likely be reciprocal effects on U.S. interests of any rule adopted in this proceeding.

Ultimately, further technological advances – some of which are in progress – will help address ICTS supply chain risk management ("SCRM") in a more targeted, durable and effective fashion. For now, we are concerned that the Proposed Rule is overly broad in ways that would inject uncertainty into the marketplace, harm the global ICT ecosystem, and hinder U.S. leadership in innovation without providing commensurate national security benefits. Its overbreadth and uncertainty of retroactive unwinding could also chill foreign companies' willingness to do business with U.S. companies. The Proposed Rule also lacks sufficient procedural safeguards in its current form, and such safeguards must be added or strengthened in any final rule.

Finally, in light of the need for significant changes to the Proposed Rule as discussed in these comments, we strongly recommend that the Department provide a further comment opportunity on a revised rule before it goes into effect. This process should be iterative, and CompTIA and our members are committed to continued engagement with the Department as this process moves forward.

DISCUSSION

I. GOVERNMENT AND INDUSTRY ARE ENGAGED IN SIGNIFICANT EFFORTS TO ENHANCE ICTS SUPPLY CHAIN RISK MANAGEMENT.

Supply chain risk management has been a key consideration for public and private stakeholders in the ICTS ecosystem for decades. Understanding that "it is impossible to completely eliminate all risks,"[4] public and private experts alike have pursued a risk management approach to enhancing supply chain security; they realize that when it comes to securing ICTS, high tides lift all boats. That said, different entities necessarily have different concerns regarding risks to their supply chains,[5] and therefore each entity has a role to play in identifying and managing its own risk. Since the technology landscape is ever-evolving and no single entity has full insight into or control over that landscape, many aspects of SCRM are an ecosystem-wide challenge, requiring industry and government to partner in pursuit of solutions.

A. The U.S. Government Has Focused Increasing Attention and Significant Resources on ICTS Supply Chain Security in Recent Years.

In recognition of evolving challenges related to new technologies and growing reliance on connectivity, efforts to enhance ICTS supply chain security have garnered significantly more attention and resources from the federal government in recent years. For example, within the last three years alone, Congress has enacted:

- the Modernizing Government Technology Act, to move federal agencies away from vulnerabilities in outdated technologies;[6]

---

[4] National Institute of Standards and Technology ("NIST"), *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, SP 800-161 (Apr. 2015), at 2, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

[5] *See generally*, NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, ver. 1.1 (Apr. 2018), at vi, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[6] National Defense Authorization Act for Fiscal Year 2018, div. A, title X, subtitle G, §§ 1076-1078, Pub. L. No. 115-91, 131 Stat. 1283, 1586 (2017).

- the SECURE Technology Act, which established the Federal Acquisition Security Council to make recommendations regarding federal SCRM standards and best practices, develop information sharing criteria, and recommend exclusion or removal orders of covered ICTS from untrusted sources from the federal supply chain;[7] and

- the Cybersecurity and Infrastructure Security Agency Act, which enabled the Department of Homeland Security ("DHS") to reorganize itself, stand up the National Risk Management Center, and launch the ICT Supply Chain Risk Management Task Force.[8]

In 2017, the President issued an Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, which among other things, directs all federal agencies to use the NIST Cybersecurity Framework and holds agency heads accountable for implementing risk management measures commensurate to the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data.[9] Globally, the United States supports the Prague Proposals which seek to, among other goals, ensure mutual commitment among signatories to appropriately manage risks to the supply chain of next generation telecommunications infrastructure.[10]

B. Public-Private Partnerships Have Made Important Contributions to ICTS Supply Chain Security, Including Through the Department of Commerce.

At the behest of federal partners, industry advisory groups have made and continue to make meaningful recommendations on enhancing security of the ICTS supply chain. The

[7] Pub. L. No. 115-390, 132 Stat. 5173 (2018).

[8] Pub. L. No. 115-278, 132 Stat. 4168 (2018); *see* CISA, *Information and Communications Technology Supply Chain Risk Management Task Force*, https://www.cisa.gov/information-and-communications-technology-ict-supply-chain-risk-management-scrm-task-force.

[9] Exec. Order 13,800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, 82 Fed. Reg. 22,391 (May 16, 2017).

[10] Govt. of the Czech Republic, *The Prague Proposals: The Chairman Statement on cyber security of communication networks in a globally digitized world*, May 3, 2019, https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/; H. Res. 575, 116th Cong. (passed by the House on Jan. 8, 2020) (endorsing the Prague Proposals).

President's National Security Telecommunications Advisory Committee ("NSTAC") produced a report on Advancing Resiliency and Fostering Innovation in the Information and Communications Technology Ecosystem last fall.[11] The Federal Communications Commission's Communications Security, Reliability, and Interoperability Council ("CSRIC") has provided recommendations on myriad aspects of ICTS risk management, including those particular to next-generation communications networks and supply chains, and was re-chartered to continue work in this vein over the next two years.[12] The Department of Homeland Security's ICT Supply Chain Risk Management Task Force provided recommendations on reducing risk posed by counterfeit ICT and fostering meaningful SCRM information sharing last summer, continues work to develop recommendations on threat categories and qualified bidder/manufacturer SCRM evaluation criteria, and plans to develop an attestation framework to communicate SCRM postures in the coming year.[13]

[11] NSTAC, *NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the Information and Communications Technology Ecosystem*, Sept. 3, 2019, https://www.dhs.gov/sites/default/files/publications/19_0916_nstac-report-to-the-president-on-advancing-resiliency.pdf.

[12] *See e.g.* CSRIC V, Working Group 6, *Secure Hardware and Software: Security-By-Design Working Group 6 – Final Report: Voluntary Security-by-Design Attestation Framework for Hardware and Software Critical to the Security of the Core Communications Network*, Sept. 2016, https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG6_Final_091416.docx; CSRIC VI, Working Group 3, *ADDENDUM to Final Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks*, Dec. 2018, https://www.fcc.gov/file/14855/download; CSRIC VII, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii (active workgroups on Managing Security Risk in the Transition to 5G (WG2) and Managing Security Risk in Emerging 5G Implementations (WG3)).

[13] Cybersecurity and Infrastructure Security Agency (CISA), ICT Supply Chain Risk Management Task Force, *Interim Report* (Sept. 2019), https://www.cisa.gov/publication/ict-scrm-task-force-interim-report.

In partnership with industry and other stakeholders, the Department of Commerce itself has advanced significant efforts: for example, the National Institute of Standards and Technology ("NIST") continues work on its foundational Risk Management Framework (NIST SP 800-37),[14] its Supply Chain Risk Management Practices for Federal Information Systems and Organizations (NIST SP 800-161),[15] and related guidance such as Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST SP 800-171).[16] The National Telecommunications and Information Administration ("NTIA") has led multi-stakeholder development of key guidance on topics such as vulnerability management, updatability and patching for the Internet of Things, and Software Component Transparency. As directed by Executive Order 13800, DHS, NIST, and NTIA led a crucial open and transparent process on enhancing resiliency against botnets and other automated and distributed threats.[17] Alongside direct efforts on SCRM, each of these processes have led to meaningful contributions in managing risks to the ICTS supply chain.

[14] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, SP 800-37 Rev. 2 (Dec. 2018), https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final. Among other things, Revision 2 integrates security-related, supply chain risk management concepts into the Risk Management Framework to address untrustworthy suppliers, insertion of counterfeits, tampering, unauthorized production, theft, insertion of malicious code, and poor manufacturing and development practices through the software development life cycle.

[15] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

[16] https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final.

[17] DHS and Dept. of Commerce, *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*, May 2018, https://csrc.nist.gov/publications/detail/white-paper/2018/05/30/enhancing-resilience-against-botnets--report-to-the-president/final.

C. Private Sector ICTS Companies are Driving Increasingly Ambitious Efforts to Secure Their Supply Chains, Including for 5G Networks.

ICTS companies themselves have strong incentives to secure their own supply chains and are increasingly driving efforts to enhance security across the connected ecosystem. As such, many entities invest in and rely on standards from bodies like the International Standards Organization ("ISO") and use non-profit models to provide technical quality and security assurance.[18] For example, the Factor Analysis of Information Risk ("FAIR") methodology provides a framework to measure, manage, and report on information risk; while the Common Criteria for Information Technology Security Evaluation ("Common Criteria") and its companion Common Methodology for Information Technology Security Evaluation enable producers of IT products to specify their security functional and assurance requirements, allow vendors to communicate the security attributes of their products, and enable testing laboratories to evaluate those products to ensure consistency with a vendor's claims.[19]

With respect to the ICTS supply chain of 5th generation wireless communications networks, industry-led efforts like the Alliance for Telecommunications Industry Solutions ("ATIS") 5G Supply Chain Standards group are working to establish end-to-end supply chain visibility, coordination of existing best practices, industry alignment with federal guidelines, and improved threat monitoring tools, among other things.[20] Groups like the O-RAN Alliance are

[18] *See, e.g.*, ISO 22301:2012 Societal security – Business continuity management systems – requirements, https://www.iso.org/standard/50038.html; ISO 27001 Information Security Management, https://www.iso.org/isoiec-27001-information-security.html; ISO 9001:2015 Quality management systems – Requirements, https://www.iso.org/standard/62085.html.

[19] FAIR Institute, https://www.fairinstitute.org/; The Common Criteria, https://www.commoncriteriaportal.org/.

[20] ATIS, *New ATIS Working Group Addresses 5G Supply Chain Standards and Development of Assured Commercial 5G Networks*, Nov. 6, 2019, https://sites.atis.org/insights/new-atis-working-

working to increase virtualization of the radio access network layer to enable increased competition, service agility, and cloud scale economics, as well as embedded intelligence to enhance security management across the network.[21]

In the long run, public-private partnerships and industry standards targeted toward risk-based models are better approaches to enhancing ICTS supply chain risk management, even if the U.S. government feels compelled to act now to address certain threats on a transactional basis. As industry and policymakers move forward, more attention will need to be given to how applications or networks may be better secured on the assumption that lower levels of the stack are insecure. Additionally, as the U.S. government continues to augment its SCRM efforts, it must continue to do so in conjunction with robust enterprise-wide programs to mitigate risk after the point of purchase, through mechanisms such as the Continuous Diagnostics and Mitigation program for civilian agencies or the Comply to Connect program through the Department of Defense.[22] While the authorities granted by the EO are exceedingly broad, the Department should not view the mission of these rules as addressing the full range of SCRM challenges in the ICTS ecosystem. Rather, it should tailor its approach to the specific gap that these authorities are best positioned and equipped to address.

---

group-addresses-5g-supply-chain-standards-and-development-of-assured-commercial-5g-networks/.

[21] O-RAN Alliance, https://www.o-ran.org/.

[22] *See, e.g.*, CISA, *Continuous Diagnostics and Mitigation (CDM)*, https://www.us-cert.gov/cdm/home; Hannah Moss, *What is Comply to Connect*, GovLoop, Feb. 28, 2019, https://www.govloop.com/what-is-comply-to-connect/.

II. PROHIBITING PRIVATE SECTOR TRANSACTIONS IS AN EXTRAORDINARY REMEDY THAT SHOULD BE USED ONLY AS A LAST RESORT.

The ICTS sector understands that supply chain risk management can have important national security implications, depending on what part of the ICTS ecosystem is being considered. However, SCRM writ large is not equivalent to national security. Every business must manage the security of the supply chains of the products and services it offers, while every enterprise, public or private, must consider and manage risk to the networks on which it relies. In addition, government entities have risk profiles that are different from private sector entities, and risk profiles also vary between entities with different missions and different levels of risk tolerance.

A. The Department Should Begin by Defining the Specific Problems to be Solved Before Applying an Extraordinary Remedy.

While government and industry often work hand-in-hand in these efforts, it is not the government's responsibility or remit to manage all ICTS supply chain risk to all entities. Instead, in approaching these issues, the government should be more specific in considering the problems it is trying to solve, so that any rules may be more tailored to address those concerns. For example, for some problems like transmitting sensitive data across untrusted networks, a 5G "secure slice" might be optimal. For general hygiene, good SCRM practices, and traceability, industry collaboration and multi-stakeholder efforts are perhaps the best route. The Department should therefore begin by defining more specifically what cannot be solved by these other efforts, and why barring or even unwinding certain private-sector transactions is the only appropriate or effective way to address those issues.

Prohibiting private sector transactions is indeed an extraordinary remedy, and narrow tailoring of any final rule authorizing that remedy is therefore essential. In contrast to the

Proposed Rule, the FCC has just recently adopted a rule prohibiting the use of *federal subsidies* on equipment from certain telecommunications suppliers of concern,[23] while Congress has recently and similarly imposed restrictions on purchases *by federal agencies* or the use of *federal dollars* in the form of grants, loans, or subsidies.[24] Against that backdrop, the Proposed Rule goes significantly further by restricting transactions between *private-sector entities* even where no federal funding is at issue. Meanwhile, the Executive Order – and in turn, the Proposed Rule – are being promulgated under the International Emergency Economic Powers Act ("IEEPA"), even as that statute makes clear that the President's authority "may only be exercised to deal with an *unusual and extraordinary threat*."[25] With both Congress and an independent agency recently choosing to avoid going as far as the Proposed Rule, the Department must be more explicit in where, why, and how this action is warranted.

In addition, the Department should not view its actions under the Proposed Rule as simply filling an "import" piece that is complementary to its recent decision to place certain telecommunications companies on the Entity List and therefore subject to *export* controls.[26]

---

[23] Report and Order, *Protecting Against National Security Threats to the Communications Supply Chain*, FCC 19-121, Docket No. 18-89 (Nov. 2019), https://docs.fcc.gov/public/attachments/FCC-19-121A1.pdf.

[24] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232 § 889(a)-(b), 132 Stat. 1636, 1917 (2018) ("FY19 NDAA Section 889"); *see also* Secure and Trusted Communications Networks Act of 2019, H.R. 4998, 116th Cong. (as passed by House, Dec. 16, 2019); United States 5G Leadership Act of 2019, S. 1625, 116th Cong. (reported favorably by S. Comm. on Commerce, Science, and Transportation).

[25] IEEPA § 202(b), 50 U.S.C. § 1701(b).

[26] Dept. of Commerce, *Addition of Entities to the Entity List*, 84 Fed. Reg. 22,961 (May 21, 2019).

Despite being issued on the same day as the Executive Order,[27] it is absolutely essential for the Department to recognize that those export controls (via Entity List designation) were imposed for a very different purpose – namely, the need to enforce U.S. laws in a situation involving potential violations of U.S. policy. In contrast, any restrictions on transactions of ICTS for use in the United States would be imposed for a very different reason – namely, the need to address specific national security risks to *U.S. networks*. These are two very different problems with different solutions, and they must not be conflated.

Finally, the Department must always bear in mind that ICTS supply chains are inherently global, with dynamic inputs that often fluctuate to accommodate economies of scale. The components in a single product may sometimes cross borders and even oceans several times before final installation by an end user. Meanwhile, other countries will be looking to the United States for leadership on these issues. The Proposed Rule risks emulation by other countries or retaliation against U.S. companies in equally vague ways, causing problems for global supply chains in general and reciprocity issues for U.S. companies in particular. For that reason, as well as those discussed above, any new authorities implemented here should only be applied to address specific national security risks, and should not be applied for political, foreign relations, or other purposes.

[27] Press Release, *Department of Commerce Announces the Addition of Huawei Technologies Co. Ltd. To the Entity List*, May 15, 2019, https://www.commerce.gov/news/press-releases/2019/05/department-commerce-announces-addition-huawei-technologies-co-ltd; *see also* Exec. Order 13,873 (adopted on May 15, 2019), https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

B. Any New Rule Should Apply Only Where Existing Legal Authorities Are Insufficient and Should Prioritize Mitigation Over Prohibition Where Practicable.

The authorities implemented by any new rule should only be used where other legal authorities or mechanisms are not sufficient to address the identified national security risk – as is, for example, required by the statute governing the Committee on Foreign Investment in the United States ("CFIUS").[28] As described in Section I above, existing programs already address many of the EO's concerns, and the Department should diligently consider objectives already achieved by these programs to issue a more narrowly tailored rule that does not overlap with existing programs and that provides US businesses with clarity and an ability to proactively mitigate ICTS national security risks. Considering the Proposed Rule through this lens will assist the Department as it considers refining the current proposal's scope (*see* Section III below). Interfering with private sector commercial transactions should be a last resort.

Mitigation vs. prohibition. In those cases where the Department determines that no other legal authorities are available to address a national security risk arising from a transaction, the Department should begin by considering mitigation, rather than blocking the transaction entirely, whenever practicable. Of course, any such mitigation needs to be effective, and the costs of mitigation and ensuring compliance cannot be excessive on the parties involved or on the government. Thus, the Rule should define and include mitigation requirements that could be imposed by the Department, as well as affirmative relief processes. This would provide businesses an opportunity to proactively implement mitigation measures, develop effective

[28] 50 U.S.C. § 4565(d)(4)(B) (President may only act after finding that other provisions of law do not provide adequate and appropriate authority).

compliance mechanisms, and provide an opportunity for relief when such measures are no longer needed.

III. THE SCOPE OF THE PROPOSED RULE IS OVERLY BROAD AND MUST BE SIGNIFICANTLY NARROWED.

As drafted, the scope of the Proposed Rule is strikingly and unworkably broad and could potentially apply to virtually every ICTS transaction or use case. For example, an individual U.S. consumer purchasing wireless speakers or a connected refrigerator for use in the home may have engaged in a transaction subject to the rule's scope. Depending on how certain terms in the current Proposed Rule are interpreted, the draft rule would potentially even provide the government foundation to ban technology products that have little-to-no national security nexus.

In its current form, the Proposed Rule fails to clearly define the proscribed activity, and by permitting transactions to be unwound after the fact, it also creates a cloud of uncertainty over every ICTS transaction, no matter how benign. When added to the nearly unlimited range of transactions and use cases to which it could apply, the combined effect is that companies will have no meaningful path to comply with the Proposed Rule. If adopted in its current form, these several and cumulative defects would likely raise legal concerns, including arbitrary and capricious claims under the Administrative Procedure Act.

In addition, while the government may have specific concerns about ICTS from certain entities, if the approach is not appropriately calibrated, the Proposed Rule's broad scope could do lasting harm to U.S. global technological leadership. The broad scope of transactions made subject to review and the nearly unlimited discretion granted to the Secretary mean that virtually all interactions between U.S. technology companies and the rest of the world risk review. In this environment, technology partners outside the U.S. may hesitate to enter into relationships with U.S. companies, for fear that those relationships could be suddenly and unexpectedly severed.

This could erode trust in buying from U.S. manufacturers, mark companies' U.S. operations as unreliable in the global marketplace, and isolate the U.S. technology sector from the rest of the world.

A. Important Terms are Used Ambiguously and Must Be Defined or Clarified.

To better tailor the scope of the Department's review, several terms in the Proposed Rule need to be defined or significantly clarified prior to the adoption of a final rule.

"Interest." The current Proposed Rule applies to 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.)"[29] As an initial matter, the term "interest" should be clarified to refer only to a present property interest. Otherwise, it could be argued that an ICT vendor retains some "interest" in its products after the product has been sold. For example, if a foreign vendor sells ICT components to an American manufacturer, who subsequently incorporates them into a smart refrigerator sold to an American consumer, the domestic retail transaction could be subject to the rule on the grounds that either the refrigerator or the components within it are property in which the foreign company retains an interest. Such an extenuated interest would not present a supply chain risk implicating national security, so the rule must be limited to those interests where the foreign vendor maintains some form of control over, or access to, the property.

Next, the contractual interests must also be clarified. The reference to contracts in the draft rule may be read expansively to include commercial agreements for termination or carriage of international data traffic or for technical arrangements necessary to effectuate international roaming of various types (voice, data, messaging) and transiting through the United States

[29] Proposed Rule § 7.1(a)(2) (emphasis added).

without interconnecting with U.S. networks. Requiring review of all such routine agreements could be unduly burdensome and is not directly related to the EO's objective.

Finally, 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.

"Dealing in" and "use." In the NPRM, the Department specifically asked for assistance in defining the key terms "dealing in" and "use."[30] To define "dealing in," the Department could look to the definitions contained in the Securities Exchange Act of 1934 for guidance. Under Section 3(a)(5) of the 1934 Act, the term "dealer" means "any person engaged in the business of buying and selling securities … for such person's own account through a broker or otherwise."[31] To borrow from this definition, "dealing in" for purposes of Executive Order 13873 could be defined as engaging directly in a financial transaction for the offering, buying, selling, or trading of prohibited ICTS. "Use" could be defined more simply as employing ICTS for its intended purpose so that unintentional use is not captured.

Other terms. We recommend providing definitions for the other terms that trigger the prohibition – "acquisition," "importation," "transfer," and "installation." To the extent that such terms are defined by other regulatory frameworks, we recommend incorporating or referencing such definitions. We also recommend that these terms be further clarified as covering only inbound transactions, as the export of ICTS is regulated by the Export Administration Regulations and other export control authorities.

[30] 84 Fed. Reg. at 65,318.

[31] Securities Exchange Act of 1934 § 3(a)(5)(A), 15 U.S.C. § 78c(a)(5)(A).

B. The Rule Must Provide Finality for Transactions and Implement a Pre-Clearance Mechanism Option.

In its current form, the Proposed Rule would allow the Secretary to unwind any transaction subject to its scope at any time before, during, or *after* the transaction occurs.[32] Thus, every future transaction of ICT products or services involving any foreign company would become inherently provisional, subject to later unwinding even years after the fact. When paired with the Proposed Rule's lack of sufficient specificity or guidance regarding which transactions would be prohibited, the cumulative effect of this retroactive review mechanism gives no guidance to companies on what activities they can proceed with and with whom they can transact business.

In at least one sense, then, the Proposed Rule as written is impossible to comply with. Without any definition of proscribed behavior, or any standards of review, this is a blanket "we will know it when we see it" action by the government.[33] In its current form, it does not give companies specific notice about its concerns yet asserts the right to prohibit or reverse such activity after the fact. Companies are left to guess what the government is concerned about. This means there is no possible company compliance program, other than to refuse to "use" any IT product or software or service that contains a single component or any nexus to a country or entity that may be deemed a "foreign adversary." And yet, the Proposed Rule does not propose to specify which countries those are. (*See* section III-D below.)

Unwinding transactions – including well after the fact – especially when companies cannot structure their conduct to avoid them, could result in an unconstitutional taking without due process. Instead of going down this path, any final rule must provide greater finality and

[32] Proposed Rule § 7.1(a)(3).

[33] *Cf. Jacobellis v. Ohio*, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

clarity, including by focusing only on pending or future transactions and by significantly narrowing the scope of transactions to which the rule applies, either through categorical exemptions or other means. Otherwise global commerce in ICTS will be massively disrupted, and U.S. economic interests will be significantly impacted.

Preclearance mechanism and advisory opinions. In its current form, the sweeping breadth of the Proposed Rule would incentivize U.S. companies to press for pre-clearances or pre-approvals for nearly every transaction – a provision not scoped in the Proposed Rule. This, in turn, creates significant commercial uncertainty for parties. Staffing and funding such a massive pre-clearance process, whereby every transaction involving the categories listed by the Department in the Proposed Rule could be submitted for a voluntary pre-clearance review, will be enormously costly both for the Department and for U.S. companies, and could become a drag on U.S. economic growth and the competitiveness of U.S. companies.

Assuming that the Proposed Rule is first significantly revised in scope as described in these comments, the Department should provide an opportunity for parties to request an advisory opinion for a contemplated transaction to provide certainty and improve compliance. In addition, establishing a voluntary preclearance mechanism could then become a helpful mechanism to promote certainty. For example, the final rule could give the Department a reasonable period to review transactions once it has been provided notice of an intended transaction by one or both parties. If the Department does not elect to review a transaction within that period, the parties could then move forward under a safe harbor.

C. The Rule Should Not Encompass Every "Foreign" Transaction and Should Specifically Exempt Subsidiaries and Extraterritorial Transactions.

The current Proposed Rule would, by its literal terms, apply to every transaction involving a non-U.S. company.[34] This is very far-reaching and goes well beyond what is contemplated in the Executive Order. It would place all foreign vendors at a fundamental disadvantage to U.S. vendors in the ICTS marketplace, even those with significant U.S. operations in their internal supply chains and those from allied nations in NATO, South Korea, Japan, etc. Enshrining such favoritism for U.S. companies into federal policy would have enormous negative consequences for U.S. companies in the global marketplace, with other countries around the world likely to implement reciprocal requirements that would harm U.S. interests.

This unfortunate outcome may be simply due to the overbroad manner in which the Proposed Rule reflects Section 1 of the EO. However, a holistic reading of Section 1 makes clear that the EO is specifically concerned with foreign *adversaries*, not every foreign government or foreign company. Specifically, although the word "foreign" does appear in isolation, that appearance comes in a sentence which itself later makes clear that it is only targeting ICTS with a connection to a foreign *adversary*.[35] Indeed, all other relevant uses of the word "foreign" in the EO's operational language are tightly coupled to the word "adversary." To address this concern, a revised rule could modify Proposed Rule § 7.1(a)(2) to cover only transactions involving a foreign adversary, rather than *all* foreign transactions. Alternatively, a

[34] Proposed Rule § 7.1(a)(2).

[35] Exec. Order 13,873 §§ 1(a) and 1(a)(i) (making clear that despite a passing mention of transactions in which a "foreign country" or a national thereof has an interest, the actual prohibition only applies to transactions connected to a "foreign adversary").

categorial exemption could be adopted for all transactions that do not involve a foreign adversary.

Subsidiaries. The phrase "subject to the jurisdiction of and direction of" a foreign adversary is exceedingly broad and could include an individual located in the territory of a foreign adversary, or the foreign branch office of a US office. The Department should consider deleting that phrase, but at a minimum the Department should recognize that subsidiaries of U.S. companies do not present the same national security risk profile. The ability of foreign adversaries to create and exploit vulnerabilities in ICTS is significantly diminished if the foreign adversary government does not have ownership or control of the parent company itself. With this in mind, transactions between a U.S. company and a foreign subsidiary of a U.S. company should be exempted from the rule's scope.

Conversely, the Department should also clarify that its intent is to focus on transactions involving foreign adversaries only where a majority or controlling interest is at issue. For example, the Department 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, the Department should consider excluding transactions involving companies "owned or controlled by" foreign adversaries when they are headquartered in an allied nation (*see* section III-D below) provided that all production of ICT occurs in an allied nation.

Extraterritoriality. The scope of the current Proposed Rule is not limited to the territorial United States, but rather extends its jurisdiction to any person subject to U.S. jurisdiction, including foreign parts of U.S.-domiciled companies. Any final rule should be limited to transactions that involve the use of ICTS in the United States. For example, the following

transactions should not fall within the rule's scope: (1) network infrastructure builds/deployments outside the United States; (2) technology deployments involving U.S. or "foreign adversary" technology conducted on a public or private network located outside of the United States; and (3) otherwise non-U.S. transactions in which a U.S. person, such as an employee, happens to be involved.

D. Greater Clarity is Needed Regarding "Foreign Adversary."

Even if the rule's scope is narrowed, companies cannot structure their conduct without some concept of which transactions will be subject to scrutiny. As a matter of due process, the Department must first presumably identify a foreign adversary before reviewing a transaction. In doing so, the Department should develop a set of criteria that can be used as a transparent guide. Moreover, the Department should focus on entities, not whole countries.

Alternatively, even if the Department maintains a country-focused approach and is reluctant to provide an exact list of which countries it considers to be "foreign adversaries," it still can and should provide *some* greater clarity regarding that designation. For example, the Secure 5G and Beyond Act, passed by the House of Representatives on January 8 of this year, and earlier advanced by the Senate Commerce Committee in 2019, specifically refers to "mutual defense treaty allies" and "strategic partners" of the United States.[36] The Department could potentially borrow those terms in crafting an exemption to the rule, given that both terms are very clearly at odds with the "adversaries" about which the EO is concerned. Other sources of specific country designations, whether inclusive or exclusive, may also be pre-existing elsewhere

[36] H.R. 2881 §§ 2(b)(2), 2(d)(4), 2(d)(6), *et al.*, 116th Cong. (passed by House on January 8, 2020); S. 893, 116th Cong. (identical in relevant part).

in U.S. laws or regulations. Ultimately, transactions involving companies organized under the laws of governments falling into those categories should be exempted from the scope of the rule.

E. The Rule Should Recognize Differences Among Use Cases by Establishing a Clear Evaluation Process and Implementing Appropriate Exemptions.

In its current form, the Proposed Rule does not differentiate between different use cases for ICTS. This is contrary to the approach recently taken by Congress in the Foreign Investment Risk Review Modernization Act of 2018 ("FIRRMA"), with the statute explicitly requiring that any determinations be based on a "risk-based analysis,"[37] and even going so far as to replace the word "threat" in the old law with the word "risk."[38] A risk-based approach makes sense, since (for example) products and services used to support a network backbone might present a very different national security risk than if products are used in edge networks or end-user applications. With this in mind, implementing some key exemptions is vital to ensuring that any final rule is targeted towards the areas of greatest concern, that the vast majority of ICTS transactions can proceed normally, and that the Department and stakeholders can utilize their limited resources effectively.

1. The Rule Should Incorporate a Clear Methodology for Criticality Assessment.

To provide clarity to the global ICTS market and direct resources where they will be most effective, the Department should incorporate and communicate a clear methodology for assessing the criticality of ICTS components in the transactions it intends to review. To that end, the Department should look to DHS for ongoing work with industry to establish a repeatable approach for assessing the criticality of ICTS components, including a calculation based on what

[37] Pub. L. No. 115-232, title XVII, § 1718(5) (2018) (codified at 50 U.S.C. § 4565(l)(4)).

[38] *Id.* § 1718(4) (modifying 50 U.S.C. § 4565(l)(3)(A)(i)).

the component is, what entity is using the component, and for what purpose. Such an approach beneficially distinguishes between an ICTS component that may be critical to national security in one context, but not in another. For example, the national security risks posed by ICT products and services used by national security agencies, other federal agencies, state and local governments, private sector critical infrastructure owners and operators, large businesses, small businesses, and individual consumers, are all different.

Similarly, the Department's methodology should account for the likelihood or actual ability of an adversary to exploit a component. For example, transactions involving components that are not logic-enabled – power supplies, fiber-optic cables, physical antennas, etc. – may fall into the definition of "information and communications technology" but should not be subject to the rule. The Department's criticality assessment should also account for mitigations available or already in place.

2. The Rule Should Exclude Transactions with No National Security Nexus and Transactions Covered by Other Processes.

In addition to a risk-based assessment process as described above, implementing certain specific exemptions at the outset could significantly reduce the number of transactions subject to the rule's scope without giving rise to any material national security risk. Like the Proposed Rule, Section 889 of the FY19 NDAA addresses national security risks related to certain telecommunications equipment and services. However, Section 889 provides two statutory exclusions: (1) a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; and (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 (i.e., telecommunications equipment that is not "logic-

enabled").[39] The Proposed Rule should incorporate similar exceptions here to both narrow the rule's scope and ensure consistency across government agencies.

Additionally, the Department should consider adopting exemptions for the following categories that either present very low risk to national security or are addressed by other federal oversight:

- Mass-market devices primarily intended for home or small office use;
- Products or transactions that are already subject to national security oversight by other agencies, or other regulatory regimes, including the CFIUS process, Team Telecom, and the Export Control Reform Act (ECRA) (*see also* Section II-B above);
- Internal transactions between a U.S.-based company and its foreign subsidiary or foreign branch offices (*see also* Section III-C above);
- Outbound transactions, particularly as these are already regulated by existing export control regimes such as the Export Administration Regulations and International Traffic in Arms Regulations (*see also* Section II-A above).

Finally, the Department should clarify that only those entities specifically under review should fall within the scope of an action under the EO. For example, end users should not be included.

IV. PROCEDURAL SAFEGUARDS MUST BE ADDED OR STRENGTHENED.

Given the significant authority the Proposed Rule would vest in the Department, the procedural safeguards in the current draft must be significantly strengthened. Indeed, Congress recently recognized the need for such protections in the similar CFIUS context when it enacted FIRRMA in 2018. The Department should implement the safeguards described below.

A. Accountability and Interagency Vetting Requirements Would Promote Responsible Use of the Department's Authority.

Even if revised in scope, the Proposed Rule would vest significant discretion in the Department. To ensure appropriate accountability for decisions made, the Proposed Rule should

[39] FY19 NDAA §§ 889(a)(2), (b)(3).

require decision-making by an appropriate senior official, following a more well-defined interagency vetting process.

Decision by senior official. As drafted, the Proposed Rule allows the Secretary to assign decision-making authority to a "designee."[40] The ultimate decision-maker within the Department should be at a politically accountable level, and delegated no lower than to a Senate-confirmed undersecretary or assistant secretary, although preferably reserved for an Under Secretary or the Deputy Secretary. This will ensure that Congress can hold the executive branch accountable for enforcement actions under Executive Order 13873, including by holding hearings and submitting requests for information from those who are subject to Senate confirmation. However, delegation below the Secretary-level for matters of process outside the final decision-making authority would be appropriate, as that would preserve room for intra-Department appeal and review.

Interagency vetting. The Department should consider establishing a more formalized interagency vetting process with defined criteria for review. The Proposed Rule merely requires that the Secretary – in determining whether a transaction is in scope and when assessing its risk – to "consult" with certain other agencies.[41] "Consultation" may be interpreted by other government agencies as basic notification, which would reduce the ability of stakeholders in other agencies to analyze transactions or to suggest mitigation structures that, from their own perspectives, would alleviate any perceived national security risk.

Moreover, the Proposed Rule grants the Department sole discretion to prohibit or not prohibit a transaction following assessment, and to assess penalties for violations, without

[40] *E.g.*, Proposed Rule § 7.2 (defining "Secretary" as "the Secretary of Commerce or the Secretary's designee").

[41] Proposed Rule § 7.101.

interagency consultation. A process whereby the heads of agencies designated in the EO are required to convene for a session, or even conduct a vote on whether a transaction is subject to the Rule, whether it poses a risk to national security, and the appropriate enforcement measures, would ensure that all interested agencies are afforded the opportunity to provide input on key decisions that will impact the critical infrastructure of the United States. The Department could look to laws governing CFIUS, which require that CFIUS voting members include Secretaries of various regulatory agencies and the Attorney General.[42]

B. The Department Should Publish Annual Reports and Regularly Share Relevant Risk Information with Appropriate Stakeholders.

At present, the rule does not require any notice by the Department to the public or even to key stakeholders. As an additional accountability measure, the Department should be required annually to publish a public report in the Federal Register on the number of transactions reviewed, blocked, and mitigated, without disclosing the names of the parties involved. The report should also describe, on an unclassified basis, and without revealing party names, the type of ICTS involved and the national security rationale for the Department's actions in each case.

In addition, to provide further clarity on the fundamental scope of this new regulatory regime, risk and vulnerability assessments utilized to inform related decision-making should be declassified and published to the greatest extent possible. If classified or highly sensitive, they should be shared with stakeholders that hold the appropriate clearances. As directed by the Executive Order, the Department of Homeland Security should establish a reoccurring, transparent, and inclusive process for producing and updating an assessment that identifies

[42] 50 U.S.C. § 4565(k)(2) (designating Secretaries as committee members); *id.* § 4565(k)(4)(A)(i) (requiring each committee member to designate an Assistant Secretary or equivalent official to carry out any delegated committee duties).

relevant entities, hardware, software, and services. The Department should also establish a process to solicit specific and constructive feedback from industry on how the specific concerns of ODNI and DHS can be addressed in a rule without overburdening industry with unnecessary uncertainty.

Doing so would allow companies to proactively take measures to avoid transactions that may be halted under the Rule. Without publishing guidance or otherwise informing businesses of the types of transactions that may be prohibited and when changes have occurred in the threat environment, companies will have no way to predict the processes or actions needed to comply with the Rule. Such guidance would also reduce the burden on the Department of rendering advisory opinions, as discussed in Section III-B above.

C. All Transaction Reviews Should Incorporate Confidentiality Protections and Provide Transparency to the Parties.

Transparency to the parties. The Proposed Rule should be modified to require that the Department provide the parties to each transaction that it elects to review with the unclassified information on which the Department's decisions are based, including with respect to decisions to open reviews, require mitigation, or prohibit transactions.

Confidentiality protections. The Proposed Rule currently states that the Secretary may consider business confidential or proprietary information as part of the evaluation of a transaction subject to Executive Order 13873. However, it contains no protections to shield sensitive proprietary or trade secret data from external review. The public would be able to access it through the FOIA process, or by the process established in the Proposed Rule whereby the Secretary will publish information summarizing decisions in the Federal Register.[43]

[43] Proposed Rule §§ 7.6, 7.103(i).

In order to fully participate in the review and potential mitigation process, businesses will need to be assured that their information will be kept confidential. The Proposed Rule should therefore be modified to describe procedures to protect business confidential information that is submitted to the Department by parties subject to reviews, to ensure that those parties have a meaningful opportunity to engage with the Department without risk that business confidential information submitted as part of the process will become public. In doing so, the Department should take care to prevent the names of parties to transactions being reviewed made public, since this could be highly prejudicial especially if mitigation measures are required.

D. Parties Should Be Given 60 Days to Respond, and the Department in Turn Should Complete Its Reviews Within 60 Days.

Opportunity to respond within 60 days. Each party to a transaction under review should have a meaningful opportunity to respond to any proposed action by the Department, including the opportunity to present business confidential information. The current 30-day timeline is too short and does not provide parties with sufficient opportunity to engage with the Department, including for example to propose mitigation. The Department should consider adopting a minimum of 60 days for the post-notification response period and review process, to allow commercial entities the ability to fully participate in the process and to establish potential mitigation methods acceptable to the government. Additional consideration and extensions should be granted for complex cases.

Prompt resolution by the Department. In its current form, the Proposed Rule would allow a review to proceed indefinitely, in the sole discretion of the Secretary. Parties to transactions under review should be assured that reviews and any other actions taken under the rule by the Department will be completed promptly and within a defined period of time. The

Proposed Rule should be modified to require a decision within 60 days after the parties submit all required information.

E. Third-Party Initiated Reviews Should be Dropped or Modified, and the Emergency Mechanism Requires Safeguards.

The Proposed Rule would allow private parties to submit information to trigger a review, and contains an emergency provision that allows the Department to dispense with most procedure in exercising its authority. In their current form, these provisions both raise due process concerns and must be eliminated or revised.

Third-party submissions. The Proposed Rule would allow private parties to submit information via a secure portal for review. The Department should eliminate this provision, or at the least require a standard or threshold for review on what type of information may be submitted by outside parties for review. To begin with, the provision is unnecessary since the Department may already review a transaction at the Secretary's discretion with or without information from a third party.

Should the submission of information by a private party nevertheless trigger the review of a transaction by the Department, the regulations should allow for the party or parties subject to the review to be provided with the information that was submitted to the Department by the outside party. The Proposed Rule should also make clear that penalties, such as those under the False Claims Act, would be applicable to any entity found submitting false reports to the Department for purposes of attempting to trigger a review.

Emergency. The emergency provision of the Proposed Rule allows the Department to dispense with most procedure in exercising its authority, and leaves the declaration of an

emergency to the Department's discretion.[44] The criteria for dispensing with the procedures are extremely broad: "when public harm is likely to occur … or national security interests require it." The Secretary – or his or her "designee" – would have virtually no accountability for such a sweeping exercise of authority, beyond simply including "the basis for the decision" in a final written determination.

Given the concerns described above regarding the need for additional procedural safeguards, the Department should build further safeguards into this emergency provision. At a minimum, the Department should adopt an appeals process for those notified of a decision under the emergency authority in order to provide an impacted entity the opportunity to respond and mitigate going forward.

V. THE DEPARTMENT SHOULD ISSUE A FURTHER NOTICE OF PROPOSED RULEMAKING BEFORE ANY FINAL RULE TAKES EFFECT.

As discussed above, this is a complex set of challenges, with major implications across nearly every sector of the U.S. economy. However, given the significant issues identified above, the current Proposed Rule would need to be significantly revised before its final adoption. For that reason, a second round of feedback would benefit both the government and industry stakeholders. Meanwhile, Congress and the President's existing emergency powers provide mechanisms to take appropriate action in response to an imminent threat to the U.S. ICTS supply chain. Therefore, there is no need for a rush to issue rules at the expense of establishing an effective and efficient process. Given the nascency of this proceeding and the implications of the authority granted in the EO, the Department should pursue an iterative development of this rule.

[44] Proposed Rule § 7.104.

CONCLUSION

CompTIA and our member companies remain committed to secure supply chains, and we appreciate that the government has an important national security interest in addressing ICTS supply chain security issues. However, in its current form the Proposed Rule is overly broad and would require significant revision as described above. We look forward to continued engagement with the Department through an iterative process in order to achieve a final result that prevents undue risks to national security while avoiding negative consequences to U.S. companies and competitiveness.

Sincerely,

/s/ Dileep Srihari

Dileep Srihari
Vice President and Senior Policy Counsel

Savannah Schaefer
Senior Director, Public Advocacy

COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION
322 4th Street NE
Washington, DC 20002

January 10, 2020