Before the
U.S. DEPARTMENT OF COMMERCE
Washington, DC 20230

In the Matter of	)	
	)	
Securing the Information and Communications	)	Docket No. 210113-0009
Technology and Services Supply Chain	)	RIN-0605-AA51

COMMENTS OF THE
TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Telecommunications Industry Association ("TIA")[1] welcomes this opportunity to comment on the Interim Final Rule ("IFR") proposed by the Department of Commerce ("Commerce") aimed at adding further security to the nation's information and communications technology and services ("ICT" or "ICTS") supply chain.[2] As both an advocacy organization and a standards-setting body, TIA represents hundreds of global manufacturers and vendors of ICT equipment and services that are supplied to the owners and operators of communications networks, enabling operations across all segments of the economy. Our member companies design, produce and sell equipment and services in countries around the world that leverage modern global supply chains, and each company has a vital stake in the outcome of Commerce's work in this proceeding. For this reason, TIA urges Commerce to consider modifications to the IFR that will correct several lingering shortcomings and allow Commerce to better balance its

[1] TIA is the leading trade association for the information and communications technology ("ICT") industry, representing companies that manufacture or supply the products and services used in global communications across all technology platforms. TIA represents its members on the full range of policy issues affecting the ICT industry and forges consensus on voluntary, industry-based standards.

[2] Interim Final Rule, 86 Fed. Reg. 4909 (Jan. 19, 2021). These comments represent the views of the TIA Public Policy Committee. While ZTE (which has been specifically identified as a prohibited supplier in other rules pertaining to supply chain security) is a member of TIA, it does not have access to the Public Policy Committee or to any of its internal communications or deliberations, and so did not influence these comments.

interest in securing the ICTS supply chain without causing needless disruption to this important sector of the economy.

As we discussed in our last comments in this proceeding, TIA believes that government policies promoting ICT supply chain security play a necessary – but by no means exclusive - role, and government-led efforts to secure the ICT supply chain need to be addressed with a coordinated, whole-of-government approach that leverages industry leadership.[3] When it comes to implementing regulations on the ICT supply chain, industry remains in the best position to create solutions to add transparency and resiliency to its supply chain, largely through the creation of industry-led standards and best practices. Where government action is necessary, this action needs to be done by working with industry to ensure that regulations are both feasible and not overly burdensome on both government regulatory administrators and companies working to comply.

TIA is appreciative of Commerce's efforts to revise their ICTS supply chain rules since the 2019 Notice of Proposed Rulemaking ("NPRM") based on industry feedback and welcomes this additional round of comments from industry before Commerce releases a Final Rule on this matter. TIA also is very supportive of the Biden Administration's acknowledgment of the critical role played by the communications and information technology sectors through the recent Executive Order mandating a government-wide review of policies impacting the ICT supply chain, including the rules issued in the recent IFR.[4] Commerce should further review and refine the IFR basked on industry feedback and stakeholder engagements while keeping that holistic, measured approach in mind.

---

[3] *See generally*Comments of the Telecomunications Industry Association, Docket No. 191119-0084 (filed Jan. 10, 2020).

[4] Executive Order on Securing the Information and Communications Technology and Services Supply Chain, (May 15, 2019).

TIA believes that some alterations to the proposed rules would enable Commerce to more efficiently administer these rules while lessening the broad financial impact on industry. Specifically, TIA would recommend Commerce do the following while reviewing these rules:

- Continue to work with industry stakeholders in order to ensure that these rules can be implemented efficiently and effectively for both industry and Commerce's staff,
- More clearly define the scope and jurisdiction of these rules so that they focus on a more narrow and critical set of ICTS transactions,
- Issue guidance to industry clarifying the conduct that would subject an ICTS transaction to Commerce's jurisdiction under these rules in order to remove the risk that everyday transactions or employment decisions could trigger a governmental review, and
- Pause the effective date of the rules until Commerce has had the chance to create a pre-licensing regime that offers trusted ICT manufacturers and suppliers to continue the critical deployment of 5G networks in the U.S. without fear of undue regulatory costs.

TIA offers these recommendations in order to continue working cooperatively and constructively with Commerce, consistent with its longstanding belief in the centrality of public-private partnerships to supply chain security.

DISCUSSION

I. Commerce needs to adopt final rules that have a narrowly defined scope of what ICT transactions would fall under the Secretary's jurisdiction and a clearer threshold for conduct that would trigger a review.

As written, the scope of ICT transactions and the threshold to trigger a review under the Secretary of Commerce's (the "Secretary") jurisdiction remains expansive. TIA appreciates Commerce's attempt to add clarity to the rules as proposed in the NPRM and define a scope of what transactions would be subject to investigation, however, the six categories laid out by the

IFR encompass practically any conceivable ICT transaction.[5] As proposed, the Secretary's jurisdiction would cover:

1. ICTS that will be used by a party to a transaction in a sector designated as critical infrastructure by Presidential Policy Directive 21 -- Critical Infrastructure Security and Resilience, including any subsectors or subsequently designated sectors;
2. software, hardware, or any other product or service integral to wireless local area networks, mobile networks, satellite payloads, satellite operations and control, cable access points, wireline access points, core networking systems, or long- and short-haul systems;
3. software, hardware, or any other product or service integral to data hosting or computing services that uses, processes, or retains, or is expected to use, process, or retain, sensitive personal data on greater than one million U.S. persons at any point over the twelve months preceding an ICTS Transaction;
4. certain ICTS products which greater than one million units have been sold to U.S. persons at any point over the twelve months prior to an ICTS Transaction;
5. software designed primarily for connecting with and communicating via the Internet that is in use by greater than one million U.S. persons at any point over the twelve months preceding an ICTS Transaction;
6. ICTS integral to artificial intelligence and machine learning, quantum key distribution, quantum computing, drones, autonomous systems, or advanced robotics.

In our discussions with members on how this rule could be practically applied to ICTS transactions, one common theme that we heard from industry is that these six categories could be construed to cover *any* existing ICTS transaction focused on building out the nation's next-generation and 5G networks – subjecting all business decisions to potential regulatory scrutiny and inevitable uncertainty. The resulting chilling effect on investment and deployment comes with real and substantial costs. According to the IFR itself, these rules would impact over 4.5 million ICTS companies and could cost a total of $20.2 billion in compliance costs to industry.[6] This huge regulatory cost on ICT companies could create a chilling effect on necessary

[5] IFR at 4913
[6] *Id.* at 4921.

transactions from trusted vendors building 5G networks. At this stage in the global push to create next-generation networks, the U.S. cannot afford to risk a chilling effect on deploying 5G networks, which industry figures show could increase the U.S. Gross Domestic Product by $1.5 trillion in the next five years and create as many as 16 million U.S. jobs.[7]

In order to reduce the uncertainty and regulatory cost to industry, the Administration should consider further ways to limit the scope of review to transactions that raise the highest concern. For instance, the purview of transactions subject to these rules could be diminished significantly if the jurisdiction were limited to transactions for critical infrastructure or involved in core networks. By focusing the scope on critical transactions, Commerce reduces the risk that the landscape of potential transactions for review will be far too broad for agency staff to administer. Streamlining the ICTS transactions applicable to review will not only limit the potential burden of regulatory costs on industry but also would ensure that Commerce's staff can review these critical transactions in the most administratively efficient manner and not get overwhelmed or sidetracked by transactions that pose little or no risk.

Additionally, the nexus of what could trigger a potential investigation under the rules as written remains extremely broad. One way to mitigate the potential transactions subject to this rule would be to further clarify what kind of conduct could be sufficient to trigger an investigation. The threshold for triggering a review in the IFR is so broad that TIA is concerned these rules could be construed to subject day-to-day decisions of a private company to government scrutiny. For example, the rules are unclear as to what nexus to a country listed by these rules as a foreign adversary would be necessary to trigger an investigation. It is feasible

[7] *See eg.* "The Impact of 5G on the United States Economy", Accenture Strategy (Feb. 22, 2021) (*available at* https://www.accenture.com/us-en/insights/high-tech/5g-economic-impact).

that these rules, as written, could be read to subject a transaction to Commerce's jurisdiction if a company involved has an employee who is a citizen from a listed country. Such a result would be a large intrusion into how a company employs staff, subject virtually every conceivable transaction to government review, and would be completely untenable in a global market such as the ICT industry.

In order to reduce risk to industry and ensure this rule can be administered effectively by agency staff, Commerce should work on creating guidance or recommendations to isolate high-risk transactions. These guidelines could be created with industry input and offer assurance to industry that day-to-day decisions, such as who the company employees would not alone subject a company's private transactions to governmental scrutiny. Such detailed guidelines, when combined with a refined scope for Commerce's jurisdiction under these rules, will aid Commerce staff by allowing them to efficiently focus on a subset of transactions that arguably require scrutiny, rather than having every ICT transaction fall under the IFR's jurisdiction. This more efficient and effective focus will ensure that Commerce has sufficient resources to review all ICTS transactions that pose a national security concern, rather than pushing resources towards transactions that pose little or no risk.

II. Commerce needs to implement a licensing system that accounts for trusted ICTS manufacturers and suppliers before these rules become effective. e.

The nation is currently in a critical stage of 5G deployment, where trusted vendors from allied nations are installing the next-generation networks that will connect America. As written, the IFR introduces substantial risks into day-to-day business operations for trusted ICT vendors and manufacturers and is expected to result in massive compliance costs for the ICTS industry,

as noted above.[8] The costs and risks to industry under the IFR comes at a time when trusted ICT vendors are already executing transactions necessary to complete next-generation networks across the nation, and could limit the ICT industry's efficiency by potentially subjecting existing transactions to review and unwinding at a later date. TIA is concerned that these rules, and their expected cost on industry, risk chilling and disincentivizing critical transactions that could enhance 5G deployment, which could put America's standing in 5G deployment at risk.

As the Administration undertakes a review of the proposed rules, TIA urges Commerce to revise the rules in order to add assurance to trusted vendors creating high-speed networks that their existing transactions will not be subject to government review. The Executive Order that originated these rules called for the Secretary to determine that certain transactions could be categorically prohibited or excluded from these rules and TIA advocated in favor of Commerce adopting such provisions in our initial comments in this docket.[9] The IFR correctly acknowledges the importance of implementing a licensing or pre-clearance system and asks for further input from industry on how this system should be implemented. TIA believes that the creation of a narrow licensing or trusted vendor system, when combined with the revisions to the scope of the rules discussed above, would allow industry to continue their critical work deploying networks nationwide while avoiding a scenario where the only path forward on an ICTS transaction ould be pre-clearance or licensing alone.

The administration could make two changes to these rules that would have an immediate impact on industry without frustrating the security goals of the IFR: suspension of the effective date until a pre-clearance or licensing structure has been imposed, and the creation of a "trusted

[8] *Supra* at (discussing the potential sweeping impact of the IFR on the ICTS community).
[9] Executive Order on Securing the Information and Communications Technology and Services Supply Chain, Section 2(b).

vendor" mechanism for preclearance. The IFR as written still subjects transactions made after January 2021 to these rules in spite of there being no established method for getting a license or pre-clearance for a transaction. The building of nation-wide next-generation networks cannot be suspended while these rules are reviewed, and subjecting existing transactions to government review before a licensing operation is set up adds too much risk and cost to the ICT industry without providing a defined and clearly defined benefit to national security interests or mitigation of existing vulnerabilities.[10] As part of the administrative review of these rules, the date for subjecting transactions to review should be pushed back a significant amount of time after a licensing system has been established.

Additionally, the Administration should create a classification for international trusted suppliers that have been building the nation's communications networks for decades. These are the suppliers currently working to close the digital divide, keep Americans connected while they work and learn remotely, and deploy 5G networks nationwide. Commerce should create a process for these trusted ICT vendors and manufacturers already hard at work in building networks in the US to be labeled as a "trusted supplier" and thus exempt from these rules, which would allow them to continue this important work. This label would not need to be permanent and could require disclosures and reporting requirements to Commerce staff in order to have companies reaffirm this designation periodically. This would allow Commerce to significantly reduce the amount of ICTS transactions that would fall under their jurisdiction to investigate, allow Commerce to focus on those transactions that truly pose a risk to the nation while adding regulatory certainty for trusted ICTS vendors and manufacturers.

[10] *See* Supra Section II.

III. **Despite the Broad Scope of the Current IFR, It Would Not Address ICTS Supply Chain Attacks Like SolarWinds.**

Recognizing the government's vital interest in protecting U.S. networks from national security threats, TIA understands the Administration's inclination to maintain every available tool to address them. In the wake of the compromise on SolarWinds' Orion software, industry and government alike feel a renewed imperative to bolster ICTS products and processes and raise the stakes for foreign adversaries seeking to exploit our networks. However, as the Department considers its own role in addressing the fallout from the SolarWinds compromise and engages in the new Administration's holistic review of these issues, it should carefully consider which tools are best suited to solve which challenges with respect to enhancing ICTS supply chain security.

The SolarWinds compromise provides a clear example of where the IFR would not prevent or remediate some of the most concerning threats to ICTS supply chains. In the case of SolarWinds, a nation state-sponsored entity modified code in the software build process, which is common across industry, using a domestic company as a vector to gain access and disguise itself as normal traffic.[11] No transaction review would have flagged this vulnerability, or rather

[11] *See* George Kurtz, *Testimony on Cybersecurity and Supply Chain Threats*, Senate Select Committee on Intelligence, at 2 (Feb. 23, 2021), https://www.intelligence.senate.gov/sites/default/files/documents/os-gkurtz-022321.pdf ("Kurtz Testimony"); Kevin Mandia, *Prepared Statement of Kevin Mandia, CEO of FireEye, Inc. before the United States Senate Select Committee on Intelligence*, at 2-3 (Feb. 23, 2021), https://www.intelligence.senate.gov/sites/default/files/documents/os-kmandia-022321.pdf ("Mandia Testimony"); Sudhakar Ramakrishna, *Written Testimony of Sudhakar Ramakrishna, Chief Executive Office, SolarWinds*, United States Senate Select Committee on Intelligence, at 3-4 (Feb. 23, 2021), https://www.intelligence.senate.gov/sites/default/files/documents/os-sramakrishna-022321.pdf ("Ramakrishna Testimony"); Brad Smith, *Strengthening the Nation's Cybersecurity: Lessons and Steps Forward Following the Attack on SolarWinds*, Senate Select Committee on Intelligence, at 2-4 (Feb. 23, 2021), https://www.intelligence.senate.gov/sites/default/files/documents/os-bsmith-022321.pdf ("Smith Testimony").

set of vulnerabilities, which only came to light because of an alert triggered by an employee's dual-factor authentication.[12]

This type of attack demonstrates the value in driving the development and adoption of industry-wide standards and best practices for security. Indeed, experts closest to the SolarWinds compromise urge industry-wide adoption of secure software design processes and enhanced collaboration between public and private sector partners, including improved information sharing, as key steps to prevent similar attacks from occurring again and to improve the United States' ability to respond when they do.[13] These kinds of assurance-based processes can more effectively illuminate ICTS supply chains so that security efforts are well-informed and nimble enough to address new threats and attacks as they evolve.

The attack on SolarWinds also underscores how important it is for the Department to clarify the scope of its IFR to specifically target the narrow circumstances under which transactional review would be effective. This can be done by adding additional processes, guidance, and a more targeted scope as discussed above.[14] To the extent companies' resources are devoted to expensive and ongoing compliance efforts such as that conceived by the currently overbroad IFR, they will incur significant opportunity cost to developing and implementing the kinds of security solutions our nation needs to fight attacks like SolarWinds. Commerce should use the opportunity of issuing a Final Rule in this proceeding to narrow this scope and provide greater insight into its goals, thus giving the ICTS industry regulatory certainty and removing

[12] *Id.*
[13] *See* Kurtz Testimony at 4; Mandia Testimony at 4-5; Ramakrishna Testimony at 4; Smith Testimony at 1, 8-14.
[14] *See infra.*at Section I.

undue compliance cost for everyday purchasing decisions, while continuing to work with industry on other solutions that could more effectively achieve security outcomes.

CONCLUSION

By working with industry to ensure that these rules are narrowly scoped and come with guidance on industry compliance, the administration will reduce national risk as resources will be put towards those transactions that pose the most risk and will ensure the efficient development of new technologies and deployment of next-generation networks. TIA welcomes this opportunity to provide input on this critical manner and will continue to participate actively in all government conversations focusing on securing the ICT supply chain. Our member companies strive every day to ensure that ICT products are both secure and reliable, and we look forward to continuing our work with Commerce and the numerous other agencies involved in this broad initiative.

By: */s/ Colin Andrews*

Colin Black Andrews
Senior Director, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 N. Courthouse Road
Suite 200
Arlington, VA 22201
(703) 907-7700

Filed: March 22, 2021