Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs	)	WC Docket No. 18-89

COMMENTS OF
THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Colin Black Andrews
Director, Government Affairs

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

February 3, 2020

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs	)	WC Docket No. 18-89

COMMENTS OF THE
TELECOMMUNICATIONS INDUSTRY ASSOCIATION

INTRODUCTION AND SUMMARY

The Telecommunications Industry Association ("TIA")[1] respectfully submits these comments in the above-captioned proceeding.[2] As both an advocacy organization and a standards-setting body, TIA represents hundreds of global manufacturers and vendors of information and communications technology ("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 mitigating the risks present in the ICT supply chain.

[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] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Report and Order, Further Notice of Proposed Rulemaking, WC Docket No. 18-89, FCC 19-121 (rel. Nov. 26, 2019) ("Report and Order" and "FNPRM"). These comments represent the views of the TIA Public Policy Committee. While ZTE (which the FCC designated as a Covered Entity in the Report and Order) 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.

As such, TIA was the leading commenter in support of the FCC's original Notice of Proposed Rulemaking[3] ("NPRM") proposing to prohibit the use of Universal Service Fund ("USF") support on equipment and services supplied by "Covered Entities." Securing the ICT supply chain will be one of the main challenges to overcome in deploying secure 5G technologies and services. Accordingly, TIA supports the FCC's actions in this docket and encourages it to proceed consistent with the recommendations set forth below.

DISCUSSION

I. AS THE TRADE ASSOCIATION REPRESENTING THE ICT SUPPLY CHAIN, TIA HAS ASSUMED A PROACTIVE LEADERSHIP ROLE IN PURSUING AND ADVOCATING FOR POLICIES THAT WILL SECURE THE NATION'S SUPPLY CHAIN WHILE PRESERVING INNOVATION.

Since filing our extensive Comments and Reply Comments in this docket supporting the adoption of rules that would guard against the acquisition and use of equipment and services in U.S. networks from suspect suppliers, TIA has been a leading and active voice on securing the supply chain in various arenas. Earlier this year, TIA officially launched an initiative to build an industry-led series of telecommunications supply chain security standards in order to aid industry and governments around the globe in assessing potential risks in the ICT supply chain.[4] TIA has also been an active thought leader in the public debate on the importance of trusted suppliers for 5G.[5]

---

[3] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Notice of Proposed Rulemaking, 33 FCC Rcd 4058 (2018).

[4] *See Trust in ICT Supply Chain Security Can Only Come from Global Industry-Driven Standards and Programs*, Jan. 21, 2020, *available at* https://tiaonline.org/what-we-do/tia-position-paper-trust-in-ict-supply-chain-security-can-only-come-from-global-industry-driven-standards-and-programs/; ***see also infra Section III.***

[5] *See, e.g.*, David Stehlin, CEO, Telecommunications Industry Association, *Telecom Industry Must Develop Trustworthy 5G Equipment Supply Chains*, BLOOMBERG LAW, Nov. 5, 2019, *available at* https://news.bloomberglaw.com/tech-and-telecom-law/insight-telecom-industry-must-develop-trustworthy-5g-equipment-supply-chains; David Stehlin, *5G Will Come With Abundant Opportunities – and some Caveats,* THE BUSINESS JOURNALS, Jan. 16, 2020, *available at* https://www.bizjournals.com/bizjournals/how-to/technology/2020/01/5g-will-come-with-abundant-

In addition, TIA has supported and advocated for legislation before Congress that would promote information-sharing regarding supply chain risks and fund the replacement of equipment in U.S. networks that could pose a national security threat. TIA has also been an active participant in the Department of Homeland Security's Supply Chain Risk Management Task Force since its inception,[6] and it remains engaged in public-private ICT sector coordinating councils focused on cybersecurity and supply chain threats. Through our active participation in these efforts, as well as input from our members who constitute the core of the industry, TIA is well positioned to advocate on behalf of effective policies to secure the nation's supply chain.

TIA's persistent focus on and interest in supply chain security is a natural extension of the ICT industry's mission. Fundamentally, the ICT industry remains focused on delivering quality products and services to its customers. Given the demonstrated risks that can flow from a compromised supply chain, no manufacturer can attest to the quality of its products without addressing the security of their supply chain. Supply chain security is thus a subset of quality and certifying the quality of ICT products is something TIA has a strong background in through our subsidiary QuestForum's TL-9000 program, which offers levels of certification for quality for ICT products.

In short, TIA speaks on these issues from the perspective of representing the ICT supply chain, standards-setting bodies, and programs that have been running for decades to ensure that ICT equipment operates at an acceptable level of quality and security.

---

opportunities-and-some.html; *see also* TIA partner event at Mobile World Congres, *The Need for Supply Chain Security in a 5G Connected World*, *available at* https://www.mwcbarcelona.com/session/the-need-for-supply-chain-security-in-a-5g-connected-world/.

[6] CISA, *Information and Communications Technology (ICT) Supply Chain Risk Management Task Force*, https://www.cisa.gov/information-and-communications-technology-ict-supply-chain-risk-management-scrm-task-force.

II. TIA STANDS BY THE WELL-ESTABLISHED RECORD IN THIS PROCEEDING AND SUPPORTS THE COMMISSION'S DETERMINATIONS REGARDING COVERED ENTITIES.

In the Report and Order, the FCC reaches a determination as to what entities should be considered Covered Entities, such that USF recipients cannot use that support for the purchase or use of their equipment and services.[7] Such a determination is not one to be made lightly by any government agency, and TIA supports the thorough, fact-based approach utilized by the FCC, which provided an opportunity for designated Covered Entities to exercise due process rights and sought feedback from industry stakeholders.

The record established in this docket in response to the NPRM is substantial. TIA's Comments and Reply Comments alone provided over two hundred pages' worth of extensive argument in favor of the designation of suppliers that raise national security concerns as Covered Entities. No new information has come to light since TIA's previous filings that would resolve the security concerns pertaining to the organizations designated in the Report and Order as Covered Entities. On the contrary, while this docket was the first official government forum to debate these security concerns, in the past year and a half, a multitude of government efforts have been launched to examine and expose threat vectors in the ICT supply chain.[8]

Even taken in isolation of other similarly focused government supply chain efforts, the present docket provides substantial evidence for the FCC to rely on in reaching a determination on what suppliers should be designated Covered Entities. TIA fully supports the FCC's adjudication in this proceeding based on the facts as they have been presented in this docket and

[7] Report and Order at ¶¶ 47-63 (designating Huawei Technologies and ZTE as Covered Entities).

[8] *See infra* Section III.A.

believes that the rules adopted in the Report and Order are an important step towards securing the nation's supply chain.

III. THE COMMISSION SHOULD TAKE A WHOLE-OF-GOVERNMENT AND WHOLE-OF-INDUSTRY APPROACH IN ADDRESSING THE ISSUES IN THE FNPRM.

The Commission is properly acting within its assigned responsibilities by promulgating rules that place conditions and restrictions on use of USF support. At the same time, the proposed rules generally reflect the Commission's recognition that it does not enjoy an exclusive mandate over these matters. In particular, TIA commends the Commission's statement supporting a "whole of government approach to supply chain security."[9] Consistent with this principle, TIA presumes that the Commission will work in close concert with its government partners to ensure that its final rules provide for meaningful, substantive, and reliable collaboration between and among different agencies, so that no relevant expertise, proceeding, or policy interest within the broader government is overlooked. The Commission's actions should account for the fact that it is not acting alone or in a regulatory vacuum in this proceeding, and that there are numerous ongoing (and probably future) government proceedings that will inform – and be informed by – how the Commission proceeds in this rulemaking.

A. Other Government Agencies Are Pursuing Activities That Bear on the FNPRM's Proposals.

TIA commends the Commission for recognizing in the FNPRM that it is not acting alone in this space, as various other government actors are pursuing concurrent initiatives that share the goal of enhancing the security of the communications supply chain. The Commission's actions here will necessarily have mutually interrelated effects with the other government activities now

[9] Report and Order ¶ 73.

underway. The FNPRM thus properly seeks comment on how the Commission can ensure that its efforts in this proceeding "are consistent and in harmony with" these other actions.[10]

As an initial matter, the Commission should (and presumably will) take full account of all related supply chain efforts in government and remain updated as to their status. In this respect, while the Report and Order's and the FNPRM's discussions of pending government activity effectively establishes the broader regulatory context, the Commission should also remain attentive to several additional pending initiatives that are directly pertinent to the proposals under consideration here:

- *Implementation of DoD Cybersecurity Maturity Model Certification.* The Department of Defense ("DoD") is currently reviewing and combining industry cybersecurity standards and best practices into one unified framework, called the "Cybersecurity Maturity Model Certification" ("CMMC") initiative.[11] Following a comment period on draft iterations of the model that spanned September through November of 2019, DoD is expected to release a final version of the CMMC (CMMC Rev. 1.0) this month, and future requests for information and for proposals at DoD will include requirements to be CMMC-certified in June and the Fall of 2020, respectively.

- *NTIA and NIST Initiatives on Supply Chain Security.* Both the National Telecommunications and Information Administration ("NTIA") and the National Institute of Standards & Technology ("NIST") are overseeing different processes to promote policies governing supply chain security and risk management – for instance, NTIA is coordinating a multistakeholder process focusing on software transparency, toward the development of a "software bill of materials."

- *Foreign Investment Risk Review Modernization Act and Export Control Reform Act.* The recent enactment of the Foreign Investment Risk Review Modernization Act ("FIRRMA") and Export Control Reform Act ("ECRA") – both of which were, like the Commission's proposed rules, specific responses to a changed national security landscape. Of particular note, FIRRMA expanded the authority of the Committee on Foreign Investment in the United States ("CFIUS") to monitor and review a broad range of transactions, even beyond the types of acquisitions and investments on which it historically had focused. FIRMMA also clarifies CFIUS's jurisdiction over transactions involving critical technology and infrastructure. The Treasury

[10] FNPRM ¶ 160.

[11] Office of the Under Secretary of Defense for Acquisition & Sustainment, *Cybersecurity Maturity Model Certification*, https://www.acq.osd.mil/cmmc/index.html (last visited Jan. 3, 2020).

Department's regulations implementing FIRRMA are scheduled to go into effect on February 13, 2020.[12]

Further, the government proceedings that the Report and Order and FNPRM do reference have evolved in critical ways in the few months since they were released:

- *Commerce Department Proposed Supply Chain Rules.* The Department Commerce has proposed rules that, if adopted, would establish a process to govern its investigation of certain transactions that may pose national security risks, pursuant to Executive Order 13873.[13] The Commission should pay careful attention to this proceeding for reasons beyond the relevance of the subject matter.[14]

    - First, TIA's understanding is that Commerce changed this proposal at the last minute to set forth proposed rules rather than "interim final rules" that would have presumptive immediate effect, as had long been expected. That shift illustrates the merit of proceeding cautiously and incrementally, while taking into account the input of industry. The Commission should heed that model as well.

    - Second, the record developed in that proceeding, which consists of filings from at least 50 different parties – including TIA, which filed substantial comments – reveals a number of widespread concerns about Commerce's proposed rules that parties recommended should and could be remedied with additional (and in some cases significant) amendments; some parties even suggested that Commerce should initiate a further rulemaking to seek comment on amended rules. Although it is not yet clear what the Commerce Department will do in light of that input, it seems clear that settling on sustainable rules for protecting supply chain security would benefit from additional public comment and engagement with industry in order to avoid undermining the very innovation that such regulation ostensibly is intended to facilitate.

    - Finally, Commerce's proposed rules specifically *require* the Commerce Secretary to consult with the FCC Chairman, among other heads of agency, in connection with transaction evaluations, and also provide the FCC Chairman the authority to request that the Commerce Secretary should undertake a transaction evaluation. These proposals in the Commerce NPRM would ensure the FCC has a role in that process and potentially allowing it to pursue certain policy goals through the

[12] U.S. Dep't of the Treasury, *CFIUS Regulations*, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-regulations (last visited Feb. 2, 2020).

[13] *Securing the Information and Communications Technology and Services Supply Chain*, 84 Fed. Reg. 65316 (Dep't of Commerce, Nov. 27, 2019); *see also* Executive Order 13873, *Securing the Information and Communications Technology and Services Supply Chain*, 84 Fed. Reg. 22689 (May 17, 2019).

[14] FNPRM ¶ 159 (seeking comment on how to proceed in light of the Commerce Department's proposals).

mechanism ultimately put in place by the Commerce Department. The Commission should therefore propose formal procedures through which it will – or will not – engage with the Commerce Department and other agencies in implementing these Commerce Department rules to allow for complementary and mutually beneficial policy action rather than duplicative or conflicting activities.

- *NDAA Section 889.* As of August 13, 2019, Section 889 of the John S. McCain National Defense Authorization Act of 2019 ("NDAA") prohibited the procurement of equipment or services from Huawei, ZTE, and others[15] by federal agency heads; as of August 13, 2020, it will also prohibit agency heads from contracting with entities that "use" such equipment or services.[16] OMB and GSA are working together to implement these government-wide bans, and those efforts will remain pertinent to the Commission's own activities. The Commission should describe (after seeking public comment if appropriate) its efforts to align its actions under this proceeding with the parallel activities that OMB and GSA are undertaking to implement those procurement restrictions. The Commission likewise must remain attuned to any changes to that implementation process prompted by a court ruling in the pending challenge to the constitutionality of Section 889.[17]

- *DHS Supply Chain Risk Management Task Force.* DHS's ICT Supply Chain Risk Management ("ICT SCRM") Task Force is a formally chartered partnership between industry and government that recently entered its second year of existence. Among its expected workstreams this year are a legal analysis and ensuing recommendations concerning the sharing of derogatory information on specific suppliers. These consensus recommendations will have obvious relevance to designations and other implementation actions under this proceeding. The Commission should act on any pertinent recommendations that the ICT SCRM Task Force proposes.[18]

- *FASC Exclusion Orders.* Related to the NDAA, the Federal Acquisition Security Council ("FASC") is authorized to issue "exclusion orders" prohibiting or removing certain contractors. The FASC has been expected to issue interim guidance on these matters in early 2020.

[15] The total list of companies listed in the NDAA were Huawei Technologies Company, ZTE Corporation, Hytera Communications Corp., Hangzhou Hikvision Digital Technology Company, Dahua Technology Company.

[16] John S. McCain National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Cong., Pub. Law 115-232, 132 Stat. 1636, § 889 (2018) ("NDAA").

[17] *Huawei Technologies USA, Inc. et al. v. United States et al.*, Civil Action No. 19-159 (E.D. Tex. filed Mar. 6, 2019).

[18] *See* Information and Communications Technology Supply Chain Risk Management Task Force, *Interim Report: Status Update on Activities and Objectives of the Task Force* (Sept. 2019).

To be sure, the ongoing nature of these activities will result in intangible synergies with the Commission's efforts given the overlap in substance and government/industry personnel working on them. But the Commission should not simply take for granted that coordination sufficient to avoid duplication of effort and conflicting outcomes will occur. Rather, TIA urges the Commission to highlight its role as a collaborator with, rather than as a competitor to, these other government actors, by expressly recognizing that these concurrent efforts are complementary to its own and will be taken into account as part of the implementation process. We recommend that any determinations the Commission may ultimately reach in this rulemaking make explicit the specific elements of other agencies' contributions to its actions here. In addition, the Commission should ensure that any final rules promulgated in this docket promote the efficient and coherent implementation of these other agency actions.

B. Any Determinations Ultimately Made by the Commission Should Be Coordinated Closely – and Must Not Conflict – With Other Related Agency Actions.

To illustrate how these broader considerations would be applied to this particular proceeding, below TIA provides high-level recommendations for the resolution of some of the key issues raised in the FNPRM.

Future determinations of "Covered Entities." Future designations of Covered Entities should rely on actions taken by Congress or on formal mechanisms for interagency and industry feedback. This inclusive approach will provide greater certainty and ensure commonality with the government's assessment of national security risks with respect to ICT. In addition, it is important that the FCC's focus remains on suppliers whose equipment that has been shown to pose a security risk, as opposed to targeting equipment solely based on where it was made. Many equipment manufacturers have deployed facilities across the globe in order to be closer to their customers, but such arrangements do not make the equipment manufactured in those

locations inherently less secure. Indeed, such manufacturers employ numerous manufacturing standards and strict quality control guidelines to preserve security.

Rip-and-replace and reimbursement. TIA supports a measured and thoughtful approach to replacing equipment from Covered Entities. The Commission should prioritize equipment that poses a threat, work with industry to develop this prioritization, and figure out how much time and what sequencing is necessary to do it in a safe, secure, and nondisruptive manner. TIA supports the creation of a reimbursement process that would allow companies to rip and replace equipment from Covered Entities; in this respect, TIA believes that the funding should come from Congress rather than from USF support.[19] TIA also recommends that the Commission consult with equipment manufacturers and "trusted suppliers" for assistance in determining a proper estimate for the total cost of the proposed reimbursement program. It is imperative that this information collection be accurate and utilize diverse sources – rather than relying solely on the carriers that would obtain reimbursement – to guarantee that the reimbursement program is sufficiently funded and that the money is appropriately distributed.

Certifications. The FNPRM asks for industry input on how USF recipients can certify that their supply chains are clear and secure. In a footnote, the Commission states in passing that manufacturers will not be required "at this time" to certify, but it specifically allows for comparable certifications to be required as a contractual matter.[20] TIA agrees that the FCC should not require industry certifications regarding supply chain security risk management, as regulatory mandates would hamper existing industry lead efforts to combat this issue. The better solution is the approach represented by TIA's recently launched initiative for industry-led

[19] FNPRM ¶¶ 143-44.

[20] Report and Order ¶ 79 n.228.

standards and best practices for supply chain security based on our QuestForum's TL-9000 program, as discussed above.

Expansion of Prohibition. The FNPRM asks whether the FCC should expand its ban to non-USF acquisitions of Covered Companies' equipment.[21] TIA believes that security risks exist regardless of how the acquisition of equipment is funded (*i.e.*, USF versus private funds), and the FCC is right to explore whether it may expand its rule to encompass the use of such equipment outside of the USF context. Fortunately, the need for the FCC to do so is mitigated by the fact that the burden does not lie on it alone; rather, Congress and other agencies are pursuing measures that will help to address security risks that do not implicate USF money.

At present, we believe the proper mechanism for Commission action outside the USF arena is a formal request from the FCC Chairman for a transaction review under the Commerce Department proposed rules, as discussed above. Again, TIA believes that the Commission should propose formal procedures through which it will – or will not – engage with the Commerce Department and other agencies in making such requests and otherwise promoting complementary and mutually beneficial policy action rather than duplicative or conflicting activities.

CONCLUSION

As it has throughout the entirety of this proceeding, TIA stands ready and willing to assist the Commission with its efforts to protect the security of communications supply chains. Indeed, our member companies strive every day to ensure that ICT products are both secure and reliable, so it goes without saying that TIA has a vital stake in the Commission's efforts. And given that membership and our extensive and continuous participation in all government conversations

[21] FNPRM ¶ 131.

focusing on securing the ICT supply chain, TIA offers an ideal nexus for bringing together and reconciling government and industry interests on these important issues. We look forward to continuing our work with the Commission and the numerous other agencies involved in this broad initiative.

By: */s/ Colin Andrews*
Colin Black Andrews
Director, Government Affairs

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

February 3, 2020