Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

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

COMMENTS OF CTIA

Thomas C. Power
Senior Vice President, General Counsel

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

John A. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200

August 31, 2020

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

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

COMMENTS OF CTIA

CTIA[1] respectfully submits comments on the Federal Communications Commission's ("Commission" or "FCC") *Supply Chain Declaratory Ruling* ("*Declaratory Ruling*") and *Second Further Notice of Proposed Rulemaking* ("*Second FNPRM*"), which continues the Commission's work on supply chain security and implements the Secure and Trusted Communications Networks Act of 2019 ("*Secure Networks Act*").[2]

I. INTRODUCTION AND SUMMARY

The Commission's *Declaratory Ruling* and *Second FNPRM* reflect the Commission's swift efforts to implement the *Secure Networks Act* and improve supply chain security. CTIA and its member companies share the Commission's commitment to protecting the U.S.

[1] CTIA – The Wireless Association® ("CTIA") (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Declaratory Ruling and Second Further Notice of Proposed Rulemaking, FCC 20-99 (July 17, 2020) ("*Declaratory Ruling*" or "*Second FNPRM*," as applicable).

communications sector's supply chain and continue to work with all government stakeholders in on-going efforts to that end.

CTIA agrees with the Commission's determination in the *Declaratory Ruling* that the codification of its *2019 Supply Chain Order* in 47 C.F.R § 54.9 "substantially implements subsection 3(a) of the Secure Networks Act."[3] In the *Second FNPRM*, the Commission is focused on further implementation of sections 2, 3, 5, and 7 of the *Secure Network Act*.[4] The centerpiece of this activity is the Commission's plan to create and "publish a list of covered communications equipment and services" ("Covered List")[5] to define the accompanying prohibition on companies' use of subsidies for such equipment or services, and to establish new reporting requirements for providers of advanced communications services. Because this is a new legal regime with potentially broad future implications for operators and manufacturers, the Commission should build enduring processes that promote predictability, are minimally burdensome, and complement broader federal supply chain efforts.

CTIA supports the Commission's proposal to prohibit the use of federal funds for communications equipment and services that are published on the Covered List and urges the Commission to tightly focus the prohibition on the use of Universal Service Funds. With respect to the Covered List, the Commission should more precisely define the "communications equipment or service[s]" and use a risk-informed approach to relevant determinations by the entities Congress has directed the Commission to rely on. In addition, process is important. The Commission must give regulated entities notice and an opportunity to adapt to additions to the

[3] Declaratory Ruling ¶ 16.

[4] *See generally*, Second FNPRM.

[5] *Id*., ¶ 29.

Covered List, so the Commission should not automatically place items on the Covered List after action by one of the "appropriate national security agencies" identified in the Act.[6] To further promote a whole-of-government approach to evolving supply chain security, the Commission should consult with the Department of Homeland Security ("DHS"), the Department of Commerce ("Commerce"), and other agencies, in addition to those mandated by Congress.

Finally, with respect to mandatory reporting, CTIA agrees that section 5 of the *Secure Networks Act* requires more information than the FCC sought in its previous collection.[7] In implementing this information collection mandate, CTIA encourages the FCC to minimize administrative burdens and provide guidelines about the "detailed justification" provision.

II. COLLABORATION BETWEEN INDUSTRY AND GOVERNMENT IS CRITICAL TO ICT SUPPLY CHAIN SECURITY.

A. The Wireless Industry Partners with Government on ICT Supply Chain Security.

A secure supply chain is critical to bring consumers next generation 5G networks and services. The supply chains for hardware, software, and services that fuel innovation in the U.S. communications sector are diverse and multi-national. Industry members are engaged with government on supply chain and cybersecurity efforts across agencies and Congress. This includes the FCC, DHS, the Bureau of Industry and Security ("BIS"), National Institute of Standards and Technology ("NIST"), the National Telecommunication and Information Administration ("NTIA"), and the Department of State ("DoS").

Several efforts, such as NIST's Cybersecurity Framework, have resulted in voluntary recommendations that help organizations adapt guidance to suit their risks and needs. CTIA was

[6] *See* Secure Networks Act § 2(c), *infra* Section II.B.

[7] *See* Second FNPRM ¶ 52.

involved at every stage of the development of the Cybersecurity Framework, including the recent iteration that expanded on "using [the] Framework for Cyber Supply Chain Risk Management."[8] CTIA will continue to engage as NIST updates its work on supply chain.

The wireless industry is a longstanding partner in DHS's work.[9] CTIA and its members represent industry on the ICT Supply Chain Risk Management Task Force ("ICT SCRM Task Force"),[10] a public-private partnership that addresses cyber threats to ICT supply chains through a "collective defense approach . . . bringing together industry and government to identify challenges and devise workable solutions" that will continue this year. CTIA supports the risk management mission of the Cybersecurity & Infrastructure Security Agency ("CISA"), which prioritizes industry partnerships. CISA recently released a 5G Strategy in which the second of five Strategic Initiatives is to "[e]xpand situational awareness of 5G supply chain risks and promote security measures."[11]

Recently, NTIA announced the Communications Supply Chain Risk Information Partnership ("C–SCRIP") to implement section 8 of the *Secure Networks Act*, which directed

---

[8] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[9] CTIA and several members are National Coordinating Center for Communications ("NCC") Industry Partners, contributing to the NCC's "continuous[] monitor[ing] [of] national and international incidents and events that may impact emergency communications." *See* National Coordinating Center for Communications, CISA https://us-cert.cisa.gov/nccic/ncc-watch (last visited Aug. 23, 2020). The industry collaborates with DHS in the Communications Information Sharing and Analysis Center ("Comm ISAC") and the Communications Sector Coordinating Council ("CSCC"). *See* Information Sharing and Awareness, CISA https://www.cisa.gov/information-sharing-and-awareness (last visited Aug. 23, 2020); Communications Sector: Charters and Membership, CISA https://www.cisa.gov/communications-sector-council-charters-and-membership (last visited Aug. 23, 2020).

[10] CTIA and member companies are active in the ICT SCRM Task Force addressing SCRM challenges. ICT SCRM Task Force Fact Sheet, DHS, https://www.cisa.gov/sites/default/files/publications/factsheet_ict-scrm_508.pdf.

[11] CISA's 5G Strategy: Ensuring the Security and Resilience of 5G Infrastructure In Our Nation, DHS, at 6 (2020) https://www.cisa.gov/sites/default/files/publications/cisa_5g_strategy_508.pdf

NTIA to establish "a program to share information regarding supply chain security risks with trusted providers of advanced communications service and trusted suppliers of communications equipment or services."[12] In its response to NTIA's request for information, CTIA encouraged it to "help the Executive Branch harmonize overlapping supply chain efforts" while "promot[ing] the sharing of actionable, verified, and timely information with a broad array of communications sector stakeholders" and "broaden[ing] participation in existing information sharing efforts rather than create a siloed approach that could fragment information sharing."[13]

Further illustrating the breadth of interest in supply chain, DoS has announced two initiatives: the 5G Clean Path initiative "to secure data traveling on 5G networks into U.S. diplomatic facilities overseas and within the United States," and the "Clean Network program" which Secretary Pompeo describes as "five new lines of effort to protect America's critical telecommunications and technology infrastructure."[14] These initiatives will depend on industry if they are to succeed in ensuring a "clean path" for "all 5G network traffic coming into and out of U.S. diplomatic facilities at home and overseas."[15]

B. The FCC Must Promote a Unified Federal Approach to ICT Supply Chain Security.

To avoid fragmentation and reach relevant stakeholders, the Federal Government must promote a unified regime for supply chain security. This will help government and industry

[12] National Telecommunications and Information Administration, Promoting the Sharing of Supply Chain Security Risk Information, 84 Fed. Reg. 35919 (June 12, 2020).

[13] Comments of CTIA, Docket No. 200609-0154, RIN: 0660-XC046 (Jul. 28, 2020) ("CTIA Section 8 Comments"). https://www.ntia.doc.gov/files/ntia/publications/7.28.20_ctia_comments.pdf

[14] *See* Press Statement, Michael R. Pompeo, Secretary Of State, Announcing the Expansion of the Clean Network to Safeguard America's Assets, (Aug. 5, 2020) https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/

[15] Department of State 5G Clean Path RFI, Request for Information, Notice ID 19AQMM20N1000, ¶ 1 (Jun. 17, 2020).

protect U.S. networks and create opportunities for strong, alternative supply chains to develop.[16] The Commission has a role in promoting a secure supply chain with other federal efforts.

Congress directed the Commission to rely on "appropriate national security agencies" when designating covered entities, equipment, or services.[17] Section 2 of the *Secure Networks Act* requires the Commission to rely "solely" on particular external determinations in creating the Covered List.[18] The *Secure Networks Act* specifies that "appropriate national security agenc[ies]" include DHS, along with the Department of Defense ("DoD") Office of the Director of National Intelligence ("ODNI"), the National Security Agency ("NSA"), and the Federal Bureau of Investigation ("FBI").[19] Thus, while the Commission has a role to play in ICT security, it must rely on relevant expert agencies.

CTIA urges the Commission to fit its supply chain activities into a whole-of-government approach, led by DHS and supported by Commerce.[20] DHS is the sector-specific agency for communications and information technology and has significant experience with national security and supply chain issues. DHS is suited to lead, especially where the implications extend beyond U.S. telecommunications carriers.[21] Commerce has authority to address national security threats. NTIA recently urged the FCC to "continue to work closely with Executive Branch entities with expertise and responsibilities concerning telecommunications security, including

[16] *See* Comments of CTIA, WC Docket No. 18-89, at 9-10 (Feb. 3, 2020) ("February Comments").

[17] Secure Networks Act § 2(c).

[18] *Id*.

[19] *Id.* § 9(2).

[20] *See e.g.*, February Comments at 9.

[21] *Id*. at 10.

supply chain security."[22] The FCC must ensure that its superintendence of the Covered List does not fragment these efforts.

III. NEW PROHIBITIONS SHOULD BE NARROW AND CONSISTENT WITH THE LIMITATIONS OF THE SECURE NETWORKS ACT.

The Commission's implementation of sections 2, 3, 5, and 7 of the *Secure Networks Act* should build on previous actions taken by the Commission, including its creation of 47 C.F.R. § 54.9.[23] The Commission proposes a new designation process for specific communications equipment and services.[24] This will result in "two different designation processes, one for the designation of an entity, as currently provided by the Commission's rules and another, more targeted process, for the designation of specific communications equipment and services per section 2 of the Secure Networks Act."[25] As the Commission acknowledges, "certain equipment or services could be subject to both the prohibition in 47 CFR § 54.9 and section 3 of the *Secure Networks Act*, and parties subject to these requirements would be responsible for complying with both prohibitions (including whichever is effective first)."[26] Given this potential overlap of regimes, it is critical that the FCC promote consistency, pursue transparency, and work with agencies that have expertise on supply chain and national security.

---

[22] Letter from Douglas W. Kinkoph, Associate Administrator, NTIA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89, at 2 (Jun. 9, 2020) ("NTIA Ex Parte").

[23] Earlier in this proceeding, CTIA and other stakeholders provided suggestions to the Commission regarding possible processes to be used for those designations—several of which have been overtaken by the *Secure Networks Act*. While CTIA remains interested in clarity and predictability in the Commission's approach to Section 54.9, the instant comments focus on the new designation regime and not on revisiting the Commission's approach to covered entities.

[24] Second FNPRM ¶ 48.

[25] *Id.*

[26] *Id.*, n. 82.

A. The Commission Should Limit New Prohibitions to the Use of USF Funds.

The entity designation prohibition adopted in the *2019 Supply Chain Order* "applies only to equipment and services in the context of USF," and not to other federal subsidies currently administered by the FCC.[27] Likewise, the new proposed equipment and services prohibition should only apply to subsidies under the FCC's USF programs.[28]

CTIA agrees with the Commission that any application of section 3 to covered communications equipment and services should rely on the same construction applied to covered entity designations in the *Declaratory Ruling*. The Commission properly reads the section 3 prohibition as "intending to apply to all universal service programs but not other Federal subsidy programs to the extent those programs may at times tangentially or indirectly involve expenditures related to the provision of advanced communications services."[29]

There is no need to expand the new prohibition to "other programs administered by the Commission that primarily support the provision of advanced communications services."[30] The Commission in the *Declaratory Ruling* concluded that that the Commission only administers two programs that qualify as a "Federal subsidy" (the USF, and the Interstate Telecommunications Relay Service Fund), that only the former "provides funds to be used for the capital expenditures

[27] 2019 Supply Chain Order ¶ 73; Declaratory Ruling ¶ 6 (describing that "[p]ursuant to . . . 47 CFR § 54.9, USF funds may not be used to purchase, maintain, improve, modify, operate, manage, or otherwise support any equipment or services produced or provided by a covered company.").

[28] Second FNPRM ¶ 48 ("To accommodate this outcome, we propose a new rule, independent of the section 54.9 prohibition, that would prohibit, going forward, the use of federal subsidies made available through a program administered by the Commission to purchase, rent, lease, otherwise obtain, or maintain any covered communications equipment and services identified and published on the Covered List. We propose that the ***new prohibition on the use of USF funds*** pursuant to the Secure Networks Act would be effective 60 days after communications equipment or services are placed on the Covered List.") (emphasis added).

[29] Second FNPRM ¶ 49.

[30] *Id.* ¶ 49.

necessary for the provision of advanced communications service," and that the Commission "believe[s] Congress clearly intended the section 3 prohibition to apply to the USF."[31]

The Commission should clarify the limits of the prohibition. Instead of clearly referencing USF support, it discusses "[a] Federal subsidy made available through a program administered by the Commission that provides funds to be used for the capital expenditures necessary for the provision of advanced communications."[32] The limitation of this prohibition to the use of USF funds should be explicitly stated in the text of the rule.

B. The Commission Should More Precisely and Narrowly Define "Covered Equipment and Services."

In defining "communications equipment or service" within the context of "advanced communications service," the Commission proposes "to include within this definition of 'communications equipment or service[s]' all equipment or services used in fixed and mobile broadband networks, provided they include or use electronic components."[33] The Commission explained its understanding "that all equipment or services that include or use electronic components can be reasonably considered essential to broadband networks," and that "the presence of electronic components provides a bright-line rule that will ease regulatory compliance and administrability."[34]

This proposed definition is unduly broad and lacks sufficient nexus to an ascertainable risk to U.S. telecommunications networks. It goes beyond the text of Section 2(b)(2), which requires that the equipment or service "pose[] an unacceptable risk to the national security of the

[31] *Id*. ¶ 20.

[32] *See* 47 C.F.R. 54.10 (as proposed).

[33] Second FNPRM ¶ 26.

[34] *Id*.

United States or the security and safety of United States persons" and be "capable of—(A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles; (B) causing the network of a provider of advanced communications service to be disrupted remotely; or (C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons."[35]

Further, it is not consistent with the risk-based approach to telecom equipment and services taken in Section 889 of the FY 2019 National Defense Authorization Act ("FY 2019 NDAA"),[36] which reflects Congress's view that some equipment poses less risk to U.S. telecom networks. Section 889 provided certain exceptions to accommodate the complex reality of global telecommunications network infrastructure. Congress excluded 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"[37] and it recognized the nature of modern telecommunications networks, which require interconnection, roaming, and backhaul using other

[35] Secure Networks Act § 2(b)(2).

[36] National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Cong., div. A, § 889 (as passed in House on May 24, 2018 by a recorded vote of 351-66) https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515rh.pdf; *see also* Defending Government Communications Act, H.R. 4747, 115th Cong. (2018), https://www.congress.gov/115/bills/hr4747/BILLS-115hr4747ih.pdf; S. 2391, 115th Cong. (2018) (Senate companion to H.R. 4747) ("FY 2019 NDAA") (prohibiting the use of all telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities) and video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities) for certain applications, such as public safety, security of government facilities, surveillance of critical infrastructure, etc.) ("FY 2019 NDAA").

[37] *Id.*

carriers' networks, and excluded from that prohibition the provision of "a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements."[38]

The Commission should take this cue from Congress and narrow the scope of the "communications equipment or service." Components and services must be assessed based on the risk their presence poses to network security; not all equipment subcomponents are essential. The Commission should, at a minimum, rely on the exceptions in Section 889 and clarify that certain equipment (such as handsets and customer premises equipment) is excluded. Moving forward, the Commission should work in established venues, such as the Communications Security, Reliability, and Interoperability Council ("CSRIC"), to develop a risk-based analysis relevant to the core layer, distribution layer, and access layer. The FCC should also develop an interagency process to collaborate with, or ensure that its work parallels, the DHS ICT SCRM. In addition to assembling an inventory of supply chain risk management efforts, the ICT SCRM launched a work stream to identify processes and criteria for threat-based evaluation of ICT supplies, products, and services.[39] These processes can inform the FCC's risk-based analysis of equipment and services for the Covered List.

The Commission should make clear that the FCC's listing of any equipment is not intended to regulate or call into question carriers' activities that connect to the facilities of a third-party, or arrangements for backhaul, roaming, or interconnection, particularly where those activities are occurring outside of the United States. This is consistent with existing policies that

[38] *Id.*, at § 889(a)(2)(A). This point has been emphasized to the Commission throughout its supply chain work. *See* Comments of USTelecom, WC Docket No. 18-89, at 7 (Nov. 16, 2018) (urging harmonization with Section 889's exceptions).

[39] CISA's ICT Supply Chain Risk Management Task Force Launches Work Streams (rev. Feb. 27, 2019), DHS, https://www.cisa.gov/cisa/news/2019/02/26/cisa-s-ict-supply-chain-risk-management-task-force-launches-work-streams.

promote commercially reasonable interconnection and roaming arrangements[40] and Section 889 of the FY2019 NDAA's exceptions. FCC equipment regulation cannot sensibly reach foreign operators' domestic equipment and preferred vendor relationships; such extraterritorial regulation would make compliance difficult, if not impossible.

C. The Commission Should Apply Risk-Based Analysis to its Use of External Determinations to Build the Covered List.

The use of external designations in creating the Covered List presents challenges. Determinations by other agencies, the Federal Acquisition Security Council ("FASC"), or DHS may focus on companies, equipment, and services that pose risks to U.S. networks, but they may not be risk-based, may not be public, may not reflect broad input, and may respond to agency concerns about economic security that are less relevant to the FCC's goals here.

In considering how to treat equipment or services identified by national security agencies or other enumerated entities, the Commission should use a risk-based assessment the type of equipment or service at issue. This will help the Commission to respond to actual and potential risks to U.S. networks and consumers as they are identified by the national security agencies. Within the FCC, the CSRIC would be an appropriate body to help design such assessments, and the FCC can further look to the DHS National Risk Management Center's EO 13873 response—developing a methodology for assessing the most critical ICT and services—to scope its approach.[41]

A principal consideration for this risk-based assessment will be how best to integrate external determinations into the Commission's designation processes. As the *Second FNPRM*

[40] *See e.g.*, 47 U.S.C. 251; § 47 CFR § 51.305 (interconnection); 47 C.F.R. § 20.12 (resale and roaming).

[41] CISA, EO 13873 Response: Methodology for Assessing the Most Critical ICT and Services (rev. Apr. 9 2020) https://www.cisa.gov/sites/default/files/publications/eo-response-methodology-for-assessing-ict_v2_508.pdf.

acknowledges, the Commission must rely on the determinations of other federal entities tasked with identifying threats to national security.[42] The Commission's risk-based analysis should include a process for prioritizing assessments based on source and the transparency of the original decisionmaker's process.

For example, the FCC is required by the *Secure Networks Act* to consider Commerce's implementation of the *2019 Supply Chain EO*.[43] This may be beneficial to the Commission where Commerce takes specific actions that identify equipment or services of concern.[44] Unfortunately, activity by Commerce under the EO will not necessarily identify particular equipment or services of concern and may raise transparency concerns described below. Already Commerce's proposed process for making determinations under the 2019 Supply Chain EO has been described as broad and unpredictable.[45] The *2019 Supply Chain EO* addresses a variety of economic, geopolitical, and national security issues and may not be an ideal input for the

[42] Secure Networks Act § 2(c) ("[T]he Commission shall place on the [Covered List] any communications equipment or service that poses an unacceptable risk to the national security…based solely on one or more of the following determinations: (1) A specific determination made by any executive branch interagency body with appropriate national security expertise, including the [FASC]…(2) A specific determination made by [Commerce] pursuant to Executive Order No. 13873…(3) The communications equipment or service being covered telecommunications equipment or services, as defined in section 889(f)(3) of the [FY 2019 NDAA]…(4) A specific determination made by an appropriate national security agency."); Second FNPRM ¶ 30-31.

[43] Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 11578 (May 15, 2019) ("2019 Supply Chain EO").

[44] Secure Networks Act § 2(c); Second FNPRM ¶ 33.

[45] *See e.g.*, Comments of CTIA, Docket No. 191119-0084, RIN 0605-AA51, at 13 (Jan. 4, 2020) ("This expansive definition is incredibly broad and would cover almost any technology. Using this definition would result in the review of a multitude of transactions, many of which would not bear on national security.") Comments of the Consumer Technology Association, Docket No. 191119-0084, RIN 0605-AA51, at 3 (Jan. 4, 2020) (cautioning that the NPRM was "breathtakingly broad, potentially covering nearly every ICTS transaction around the globe."); Comments of IBM Corporation, Docket No. 191119-0084, RIN 0605-AA51, at 1 (Jan. 4, 2020) (commenting that the proposed rules were "massively overbroad" and if enacted in their current form, "would harm the U.S. economy, fail to enhance U.S. national security, and violate principles of due process.").

Covered List. Before adding any equipment or services to the Covered List in response to Commerce action under *2019 Supply Chain EO*, the FCC should develop its own record to establish specific findings on each component or service implicated by Commerce action.[46]

The *Second FNPRM* notes that Congress directs the FCC to consider the work of the FASC on "criteria and processes for assessing threats and vulnerabilities to the supply chain posed by the acquisition of information technology" and inquires how the efforts of this body and of other similarly tasked committees should be weighted in Commission decision-making.[47] CTIA encourages the Commission to consider all of the outputs of these committees in a risk-informed manner and make relevant determinations about specific equipment available for public comment, as further explained in Section IV.B. below

By contrast, the FCC may not find reliance on the Committee on Foreign Investment in the United States ("CFIUS") or Team Telecom proceedings to be as helpful, because these proceedings tend to focus on operational and governance issues related to foreign investment.[48] Team Telecom and CFIUS are not structured to make determinations of general supply chain risk. Their work is non-public and may not help inform Commission determinations about the risk posed by particular equipment or services. The Commission can look to these bodies for information sharing about emergent areas of concern, but mitigation agreements or transaction conditions are unlikely to provide the sort of determinations that should inform risk-based additions of particular equipment to the Covered List.

[46] 2019 Supply Chain EO.

[47] Second FNPRM ¶ 32.

[48] *Id.*

The FCC should consider the work of the Federal Acquisition Regulatory ("FAR") Council and DoD with respect to FY 2019 NDAA Section 889 and its carve-outs. The FY 2019 NDAA's Section 889 expressly excludes from its procurement ban some categories of equipment, including all equipment that is incapable of "rout[ing] or redirect[ing] user data traffic, or which do[es] not provide visibility into user data," as well as certain services, including "backhaul, roaming, and interconnection."[49] The Commission should give due consideration to the FY 2019 NDAA's enumerated exclusions of equipment and services as a strong signal that the Congress did not intend to prohibit routine commercial interactions that facilitate the transit and completion of global traffic. To that end, the FCC should consider USTelecom's recommendation to include a "criticality assessment, consistent with Congressional intent, when determining covered equipment in order to maximize the benefit to the security of our nation's networks."[50]

IV. TRANSPARENCY AND NOTICE SHOULD DRIVE IMPLEMENTATION OF THE SECURE NETWORKS ACT AND DESIGNATIONS FOR THE COVERED LIST

A. Predictability is Critical to Building Reliable Supply Chains and Secure Networks.

The *Second FNPRM* seeks comment on several proposals to develop the Commission's processes for designating entities, equipment, and services for inclusion on the Covered List as real or potential risks to U.S. telecommunications networks or consumers. Any processes the

[49] *See* FY 2019 NDAA § 889(a)(2); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs et al*., WC Docket No. 18-89 et al., Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423, ¶ 70, n. 209 (2019); *see also* comments of USTelecom – The Broadband Association, PS Docket No. 19-351 et. al. (Mar. 27, 2020) (noting that "[a]dopting a definition that comports with both Acts—one that does not apply to layer one and layer two equipment—follows the direction in the Secure Networks Act and with the 2019 NDAA.").

[50] *Id*. at 5.

Commission adopts to implement the *Secure Networks Act* must be open and transparent. Supply chain decisions and operations are highly complex and are the result of long-term planning. Ensuring that any decisions regarding potential changes to the supply chain are made in coordination with industry can help mitigate harms.

B. The FCC's Reliance on Other Agencies' Determinations Needs To Be Transparent, Because Some Agency Designations May Not be Public and Prohibitions Take Effect Within Sixty Days of Designation.

To avoid surprise and exorbitant sunk costs, the Commission must maintain a robust and transparent process for regulated entities. The FCC should use caution that it is only incorporating determinations that are sufficiently precise to be defensible in public proceedings; it should not rely on informal or secret determinations by other agencies. Nor should the Commission automatically add to the Covered List upon a finding by another agency. It should provide notice of additions or changes to the Covered List.

The Commission needs to provide notice of designations prior to inclusion, modification, or removal from the Covered List. The fact that another agency's determination may have been publicly released[51] is not justification for dispensing with public notice and opportunity to comment. Other agencies' determinations may not have benefitted from public input or may have processes that are less accessible to or understood by all entities that will be impacted.

Of the determinations the Commission must rely upon under section 3(c) of the *Secure Networks Act*,[52] several are not transparent and thus should not result in automatic listing of items on the Covered List. As discussed, Commerce's implementation of the *2019 Supply Chain*

[51] Second FNPRM ¶ 38 (proposing that the Commission would not be required to publish a public notice when it receives "any determinations covered under sections 2(c)…publicly released by the original decisionmaker.").

[52] *See supra* n. 42.

EO is replete with concerns about breadth and unpredictability;[53] the FASC does not operate in a public fashion, and does not solicit public input; and implementation of the NDAA may or may not result in a list of entities that are off limits to the federal government, but that process is subject to uncertainty and waivers that are not publicized in a coordinated way.

By contrast, the FCC, as an independent agency, is governed by important expectations for administrative rigor and transparency. Its designations will have distinct legal consequences in several areas, including for the use of federal funds, compliance and auditing obligations, design of networks, and the nature of supplier relationships. Although determinations by other agencies with national security expertise are relevant, the regulated community should be given adequate notice and an opportunity to evaluate the basis for any FCC decisions.

Notice is critical here because the multiplicity of activities may be challenging for diverse USF recipients to track and monitor. Smaller entities may not track proceedings before every agency, but they should be provided every reasonable opportunity to comment prior to a consequential change being made to the established supply chain. This challenge is all the more critical because section 3 of the *Secure Networks Act* provides that the prohibition will take effect "60 days after the date the Commission places such equipment or service on the list."[54] By seeking public comment, rather than automatically placing equipment or services on a list, the Commission would be able to limit unfair surprise to the regulated community and disruption in federal USF programs and compliance. This would also ensure that USF recipients have a reliable source to consult for current and imminent FCC-related obligations.

[53] *See supra* n. 45.

[54] Secure Networks Act § 3.

C. The Commission Should Consider Confidential Mechanisms to Provide the Regulated Community Guidance As Needed.

While transparency and notice are critical to ensuring timely and actionable supply chain decisions for the industry writ large, some company-specific issues may require a process by which to seek and obtain Commission guidance on a confidential basis. The process of designating entities, equipment, and services for inclusion on the Covered List, especially in the early and transitional stages, will prompt company-specific requests for guidance. Supply chain options and decisions are often proprietary and highly confidential, making it fraught for a company publicly solicit Commission input on a potential business partner or vendor. CTIA encourages the FCC to explore varied approaches, in addition to formal declaratory rulings, to provide guidance that can give the regulated community confidence in their decisions.

D. The Commission's Process Should Recognize Reasonable Reliance and Provide Regulatory Certainty to Promote Maintenance of Telecommunications Networks.

As the Commission is well aware, the deployment of advanced telecommunications networks takes years, and networks then are maintained and upgraded over the course of decades. This requires network operators and their vendors to have access to a steady and predictable supply chain over a prolonged period of time. Even minor changes to the availability of a vendor, piece of equipment, or a service can have costly repercussions.

To promote predictability in business planning and to minimize disruptions from additions to the Covered List, CTIA encourages the Commission to permit grandfathering some existing contracts.[55] Historically, the Commission been wary of taking regulatory action that upends reasonable reliance interests or retroactively calls into question third party contracts,[56]

[55] Second FNPRM ¶ 50.

[56] *See e.g., Amendment of Parts 2, 21, 74 and 94 of the Commission's Rules and Regulations in regard to frequency allocation to the Instructional Television Fixed Service, the Multipoint Distribution Service,*

and the Commission has grandfathered business arrangements were new obligations are unduly disruptive or inconsistent with other policy goals.[57] Given the variations in types or sources of equipment that may be at issue in the future, the Commission should not try to define too many requirements *ex ante* for the kinds of arrangements that qualify for grandfathering.[58] Rather, the FCC should exercise its discretion and work with the regulated community to build in permissible grandfathering that is consistent with fair process and sensible regulatory practice.

Predictability also includes ensuring that the Covered List is maintained with timely and actionable information. It is not clear from the language of section 2(d) of the *Secure Networks Act* that the Commission is precluded from updating the Covered List beyond specific statutorily-mandated updates.[59] Therefore, the Commission should adhere to familiar administrative law principles and act in a manner that is reasonable, rational, and not arbitrary or capricious.[60] If an intervening event occurs to warrant a revision of the Covered List between statutorily-mandated updates, the Commission should not hesitate to follow an open and transparent process pursuant to its authority under the Administrative Procedures Act. This will ensure that Covered List remains an accurate source of useful information.

---

and the Private Operational Fixed Microwave Service, Memorandum Opinion and Order on Reconsideration, 98 FCC 2d 129, 133 ¶ 14 (1983) (holding that "[f]or the public, grandfathering provisions protect against disruptions in existing services. For the operating station, grandfathering guards against economic dislocation and protects the reliance interest of the station in the spectrum as allocated.")

[57] *See e.g.*, Section 63.71 Application of MCI Communications Services, Inc. d/b/a Verizon Business Services for Authority to Discontinue Domestic Telecommunications Services, Order, 29 FCC Rcd 9670 (rel. Aug. 12, 2014) (granting Verizon Business Services authority to grandfather its private line DS0 services pursuant to section 214(a) of the Act and section 63.71 of the Commission's rules); *FCC v. National Citizens Committee*, 436 U.S. 775, 803 (1978) (upholding the FCC's decision to grandfather certain combinations on the basis that it reflected "a rational weighing of competing policies.")

[58] Second FNPRM ¶ 50.

[59] *Id*. ¶ 45.

[60] *United States v. Mead Corp*., 533 U.S. 218, 227 (2001).

V. REPORTING OBLIGATIONS SHOULD BE MINIMALLY BURDENSOME

A. The Commission Should Implement the Secure Networks Act in a Manner that Minimizes Reporting Burdens.

Section 5 of the *Secure Networks Act* requires each "provider of advanced communications service" that has "purchased, rented, leased, or otherwise obtained any covered communications equipment or service" after August 14, 2018, must submit an annual report, "in a form to be determined by the Commission."[61] The section 5 requirements also prescribe that the provider include a "detailed justification" for procuring such communications equipment or services, exceeding the scope of the previous Commission information collection.[62] In implementing section 5, CTIA urges the Commission to conduct information collections that are consistent with long-standing policy, and are minimally burdensome on reporting entities.

CTIA agrees with the Commission that a requirement that filers report the type, location, date obtained, and any removal and replacement plans of covered equipment and services in their network would be straightforward and not unduly burdensome. The Commission should provide guidance as to the requirements for a "detailed justification," as the provision could create a significant amount of uncertainty among filers.

B. The Commission Should Protect Proprietary and Confidential Information from Public and Other Disclosures.

The Commission should treat information provided in response to its collection requirements as presumptively confidential and not subject to routine public inspection. This presumption should extend beyond provider-specific information regarding the location of covered equipment, and also include the individual provider's contribution to the "magnitude of

[61] Secure Networks Act § 5; Second FNPRM ¶ 52.

[62] *Id.*

covered equipment and services" in U.S. networks.[63] While the aggregate quantity of covered equipment and services in U.S. networks may be relevant to the public, it is not as clear that provider-specific information is of similar value. Given the breadth of the Commission's definition of "communications equipment or service"—which may reach any electronic components—these disclosures are likely to be more expansive than helpful.

VI. CONCLUSION

For the foregoing reasons, the Commission should approach any final decision in this proceeding with an emphasis on predictability and transparency and in coordination with other expert agencies.

Respectfully submitted,

/s/ Melanie K. Tiano

Melanie K. Tiano
Director, Cybersecurity and Privacy

Thomas C. Power
Senior Vice President, General Counsel

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

John A. Marinho
Vice President, Technology and Cybersecurity

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

August 31, 2020

[63] *Id.* ¶ 56.