Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 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
NCTA – THE INTERNET & TELEVISION ASSOCIATION

Rick Chessen
Loretta Polk
National Cable & Telecommunications Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431

June 1, 2018

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 NCTA – THE INTERNET & TELEVISION ASSOCIATION

NCTA – The Internet & Television Association (NCTA)[1] submits these comments in response to the Commission's Notice of Proposed Rulemaking (NPRM) in the above-captioned proceeding.[2] The Notice seeks comment on proposed rules prohibiting the use of money from the Universal Service Fund (USF) to purchase equipment or services from providers identified as posing a national security risk to communications networks or the communications supply chain.

INTRODUCTION AND SUMMARY

Concerns about state-sponsored malicious actors exploiting supply chain vulnerabilities for purposes of intellectual property theft, surveillance and espionage – and even incapacitation of critical infrastructure and industrial control systems – have emerged as a prominent national and economic security issue.[3] While the supply chain security and integrity objectives driving this proceeding are important, the Commission's proposal to adopt rules under the Universal

---

1 NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving approximately 85 percent of the nation's cable television households and more than 200 cable program networks. The cable industry is the nation's largest provider of broadband service after investing more than $250 billion over the last two decades to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to more than 30 million customers.

2 *In re Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Notice of Proposed Rulemaking, WC Docket No. 18-89, FCC 18-42 (rel. Apr. 18, 2018) (*NPRM* or Notice).

3 *See, e.g.*, Letter from Tom Cotton, U.S Senator, et. al to Ajit Pai, Chairman, FCC (dated Dec. 20, 2017), https://docs.fcc.gov/public/attachments/DOC-349859A2.pdf.

Service Fund support program should be considered in that broader context. In the Notice, the Commission recognizes a range of existing laws and ongoing actions in the Executive Branch and Congress aimed at safeguarding and securing communications networks and other essential systems. As discussed below, this objective would be best served by a coordinated, "whole of government" approach in which the Commission's targeted efforts in the USF context are one part of a broader holistic, cross-sector interagency effort that includes initiatives pursued by the Department of Homeland Security (DHS) and the Department of Commerce addressing cybersecurity issues.

Further, the Commission also should take into account any potential adverse effects that adopting new rules may have on communications network equipment pricing, competition, and innovation. A cost-benefit analysis is crucial to achieving the goal of managing supply chain risks without undue economic harm and without unintended and unwanted consequences.

If the Commission opts to act unilaterally, it should clarify the boundaries of the rules' application to provide companies with certainty regarding the assessment, determination, identity, and scope of black-listed equipment and services. The Commission also should address key definitional issues, as well as practical and operational concerns, such as the grandfathering of already-deployed equipment obtained from subsequently prohibited suppliers, the treatment of contractors and sub-contractors, and the competitive impact of the proposed rules on product, cost, and service upgrades for existing equipment. In addition, the Commission should make clear that the legal basis for any rules it adopts in this proceeding stems from its authority, as the administrator of the USF program, to impose conditions and restrictions on the receipt of program monies, rather than any sort of plenary authority over the communications network supply chain.

Finally, the government-industry collaboration that is necessary to address these concerns will require processes that allow private sector companies to engage with the government in candid partnership, without fear that this well-intended engagement will expose them to new legal, regulatory, or business risks. This will require application of DHS's statutory confidentiality protections provided under the Protected Critical Infrastructure Information (PCII) program[4] to engagements between companies and government in connection with risk assessments, as recommended in 2015 by the Commission's Communications Security, Reliability and Interoperability Council (CSRIC) in a major report on Cybersecurity Risk Management and Best Practices.[5] The Commission should promote these CSRIC recommendations in its coordination with DHS on these issues.

I. NCTA MEMBERS RECOGNIZE THE IMPORTANCE OF SUPPLY CHAIN SECURITY AND MAKE SIGNIFICANT INVESTMENTS TO ENSURE THE SECURITY AND INTEGRITY OF THEIR NETWORK EQUIPMENT

The cable industry and the communications sector as a whole have long recognized the importance of supply chain security. Ensuring the security of the network supply chain is a fundamental business imperative for NCTA members. The marketplace consequences of poor supply chain security – in terms of loss of trust and damage to reputation – offer network providers ample incentive to ensure the integrity of their equipment supply chain.

Cable operators are in the business of providing their customers with a safe, secure and reliable connection to the Internet and other communications services, and therefore have strong business incentives regarding cybersecurity and supply chain security. Operators implement

---

4 DEP'T OF HOMELAND SEC., *Protected Critical Infrastructure Information Program*, https://www.dhs.gov/pcii-program (last visited May 31, 2018).

5 *See* CSRIC IV, *Cybersecurity Risk Management and Best Practices - Working Group 4 Final Report*, at 6 (Mar. 2015), https://transition fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf (calling for "company-specific meetings" with the Commission and DHS under PCII protections).

robust internal protocols and procedures to ensure product integrity in critical infrastructure network assets and applications. Operators have programs to assess risk associated with third parties connected to their network and those that process information. Programs focus on aspects like service availability risk and information protection, such as Payment Card Industry (PCI) compliance standards. Risk assessment may include, for example, the impact of third party service disruptions on operations, which informs agreed-upon recovery time objectives. Vendors (or suppliers) are required to maintain Business Continuity, Disaster Recovery, and Incident Management plans. These requirements are enforced through service level agreements (SLAs). Operators also carefully review the security practices of the vendors they hire, and also monitor ongoing performance to ensure that vendors continue to satisfy the operators' security requirements. All of this in combination with implementing the new guidance on supply chain risk management (SCRM) from the newly updated National Institute of Standards and Technology (NIST) Cybersecurity Framework Version 1.1 and related NIST guidance will further strengthen efforts to maintain the security and integrity of network assets deployed by cable operators.[6]

The cable industry's research and development arm, CableLabs, has a robust equipment certification program that tests and certifies certain devices manufactured by third parties.[7] Working with cable operators and cable equipment manufacturers, CableLabs has developed

---

[6] NIST provides guidance to federal agencies on a wide variety of cybersecurity issues, including SCRM. *See* NAT'L INST. OF STANDARDS AND TECH., *Framework for Improving Critical Infrastructure Cybersecurity - Version 1.1* (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Additionally, NIST has conducted case studies of industry best practices on SCRM. *See* NAT'L INST. OF STANDARDS AND TECH., *Cyber Supply Chain Risk Management - Cyber Supply Chain Risk Management*, https://csrc nist.gov/ Projects/Supply-Chain-Risk-Management/Best-Practices (last visited May 31, 2018).

[7] *See* CableLabs, About CableLabs, https://www.cablelabs.com/about-cablelabs/ (last visited May 31, 2018). Cable operators and their suppliers use a variety of third-parties for supply chain integrity, such as Underwriters Laboratories for equipment safety specifications and testing, ASTM for power pole specifications, and CableLabs for DOCSIS device specifications.

various specifications to facilitate the manufacturing of interoperable cable devices used in cable networks. The testing and certification CableLabs conducts for devices manufactured by third parties is focused on compliance to CableLabs' interface specifications, such as its DOCSIS specification.[8] This certification process ensures that CableLabs certified devices are interoperable and conform to the specification's security requirements, including the use of digital certificates issued from CableLabs' public key infrastructure (PKI). For example, the digital certificates provide a unique, immutable, and attestable digital identity for each cable modem and cable modem termination system (CMTS) on the cable operator's network. Cable operators use the digital certificates to authenticate cable modems on their network, to ensure secure software updates from the device manufacturer or the cable operator, and to encrypt broadband traffic between the cable modem and CMTS.[9] The use of digital certificates dramatically reduces the possibility of fraudulent cable modems on a cable operator's network.

Through partnerships with other stakeholders in the communications sector, cable operators also participate in collaborative supply chain security efforts undertaken by the Communications Sector Coordinating Council (CSCC) and the Commission's Communications Security, Reliability, and Interoperability Council (CSRIC). The Communications Sector's Supply Chain Working Group has evaluated and recommended practices, risk mitigation opportunities, and coordinated approaches to institutionalizing effective SCRM efforts across the

---

[8] CableLabs' certification process is focused on ensuring conformity with its interface specifications, which only govern the interaction between cable network components (e.g., cable modem and CMTS), rather than the internal architecture or software implementation of the particular network component. CableLabs' testing does not directly or fully evaluate a vendor's development of software or its use of software in a network component.

[9] CableLabs, *Security Networks in the Broadband Age*, at 5-9 (Spring 2017), https://www.cablelabs.com/wp-content/uploads/2017/04/Securing-Networks-in-the-Broadband-Age-2017.pdf. Digital certificates help ensure only the source of a software update as provided by the device manufacturer.

sector.[10] As the NPRM notes, CSRIC VI currently is evaluating strategies and practices for reducing "risks to network reliability and security, including mechanisms to best design and deploy 5G networks to mitigate risks to network reliability and security posed by, among other things, vulnerable supply chain."[11] These efforts follow prior CSRIC supply chain related initiatives,[12] and offer an array of recommended protocols and practices for mitigating supply chain risks. In short, there are existing government-industry initiatives underway to address these concerns, and any Commission action or future government activities should build on these initiatives and avoid inconsistent approaches.

II. THE COMMISSION SHOULD SUPPORT A HOLISTIC APPROACH TO FEDERAL SUPPLY CHAIN SECURITY POLICY

Ensuring the security of global supply chains for information and communications technology (ICT) products and services is an extraordinarily complex undertaking with wide-ranging impacts on key areas such as the economy, national security, trade policy, innovation, and technological advancement in an interconnected and interdependent global ecosystem. The supply chains for communications networks are diverse and interdependent. They encompass intellectual property development, component and chip fabrication, device assembly and testing, software and hardware, device installation and management, and routing and managing of data and services over those networks.[13]

---

[10] DEP'T OF HOMELAND SEC., *Communications Sector-Specific Plan - An Annex to the NIPP 2013*, at 21 (2015), https://www.dhs.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf.

[11] *NPRM* ¶ 9. *See* FCC – Communications Security Reliability and Interoperability Council, *CSRIC VI Working Group Descriptions*, at 3 (Feb. 2, 2018), www.fcc.gov/files/csric6wgdescriptions2-2018.pdf.

[12] *See* FCC – Communications Security Reliability and Interoperability Council, *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*, at A-6 (Sept. 2016), (examining frameworks useful for self-assessment against the 11 recommended best practices for communications sector members to use to assess and manage supply chain cybersecurity risk).

[13] *See Telecommunications, Global Competitiveness, and National Security: Hearing Before the House Energy and Commerce Committee - Subcommittee on Communications and Technology*, 115th Cong. (May 16, 2018)

Ensuring Coordinated Efforts of Multiple Agencies and Congress. The breadth and complexity of issues implicated by efforts to advance communications supply chain security warrant a well-coordinated "whole of government" response that should include: DHS; the Commerce, Justice, and Defense Departments; the intelligence community; and sectoral regulators like the FCC.

DHS, the Sector Specific Agency for both the communications and the IT sectors, plays a key role in coordinating Federal agency efforts on cybersecurity, including supply chain security, and is well-positioned to coordinate the government's interagency efforts on these matters. The Department's recently announced cybersecurity strategy emphasized the interdependent nature of supply chain risks, noting that effective policies in this area require the government to "partner with information technology, communications, cybersecurity services, and other communities" such as cloud providers.[14] To that end, DHS has established a Cyber Supply Chain Risk Management (C-SCRM) initiative, which evolved through the Department's collaboration with the Department of Defense and the intelligence community and is designed to "identify and mitigate supply chain threats and vulnerabilities to High Value Assets."[15] In conjunction with

(referencing to the testimony of Dr. Charles Clancy, Professor of Electrical and Computer Engineering, Virginia Tech, at 1).

[14] *See* DEP'T OF HOMELAND SEC., *Department of Homeland Security Cybersecurity Strategy*, at 23 (May 15, 2018), https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf. DHS's strategic approach to bolstering network resilience calls for leveraging the Department's "unique expertise" to develop "solutions to identify and manage supply chain risks for federal networks and other national and global stakeholders." *Id.*

[15] *See State of Play: Federal IT in 2018*: *Hearing Before the House Committee on Energy & Commerce - Subcommittee on Information Technology, Committee on Oversight and Government Reform*, 115th Cong. (Mar. 14, 2018) (statement for the record of Jeanette Manfra, Asst. Sec'y. for Cybersecurity and Commc'ns., Nat'l Protection and Programs Directorate, Dep't of Homeland Sec.) . *See also* Lauren C. Williams, *DHS Developing Supply Chain Security Initiative*, FCW, (Feb. 14, 2018), https://fcw.com/ articles/ 2018/02/14/dhs-supply-chain-security.aspx; Jory Heckman, *DHS, Lawmakers Doubling Down on Supply Chain Risk Management*, Federal News Radio (Feb. 15, 2018), https://federalnewsradio.com/cybersecur ity/2018/02/dhs-lawmakers-doubling-down-on-supply-chain-risk-management/.

those efforts, DHS recently launched a two-pronged initiative to address both general and targeted supply chain risks, with a specific focus on the telecommunications sector.[16]

The Commerce Department also has been actively involved in efforts to mitigate state-sponsored national security risks from overseas communications equipment vendors, and is well-suited to promote private sector engagement with the government in developing supply chain security solutions.[17] For over a decade, the Federal standards-setting body within the Commerce Department, NIST, has been involved in SCRM efforts on behalf of Federal agencies in connection with their acquisition of information technology and communications infrastructure.[18] NIST also recently updated the Cybersecurity Framework to provide SCRM guidance.[19] Framework Version 1.1's new SCRM guidance was designed to help organizations identify, assess, and mitigate security risks arising from technology-related products and services that may contain potentially malicious functionality or vulnerabilities. The NIST guidance addressed areas such as supplier selection and controls, assessing and verifying vendor

---

16 Tim Starks, *DHS tackles systemic cyber risk, supply chain threats*, POLITICO (May 7, 2018), https://www.politico.com/newsletters/morning-cybersecurity/2018/05/07/dhs-tackles-systemic-cyber-risk-supply-chain-threats-205953. *See also*, *House Energy and Commerce Subcommittee on Communications and Technology Hearing on Telecommunications, Global Competitiveness, and National Security* (May 16, 2018) (statement of Clete Johnson, Partner, Wilkinson Barker Knauer, LLP, at 4) (noting commencement of "Telecommunications Supply Chain Risk Assessments by DHS's Office of Cyber and Infrastructure Analysis").

17 *See, e.g.*, Mariam Baksh, *Commerce Dept. Order Could Shut ZTE Out of U.S. Market as FCC Votes on Supply-Chain Proposal*, Inside Cybersecurity (Apr. 17, 2018), https://insidecybersecurity.com/daily-news/commerce-dept-order-could-shut-zte-out-us-market-fcc-votes-supply-chain-proposal; Ali Breland, *Commerce Bars U.S. companies from selling to ZTE*, THE HILL (Apr. 16, 2018), http://thehill.com/policy/technology/383392-commerce-bars-us-companies-from-selling-to-zte.

18 NAT'L INST. OF STANDARDS AND TECH., *Information and Communications Technology Supply Chain Risk Management*, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Managements/documents/nist_ict-scrm_fact-sheet.pdf (noting that NIST "is responsible for developing standards, guidelines, tests, and metrics for the protection of non-national security federal information and communications infrastructure" and has worked with the Department of Defense to develop "supply chain tools, resources and risk management practices, in partnership with industry").

19 NAT'L INST. OF STANDARDS AND TECH., *Framework for Improving Critical Infrastructure Cybersecurity - Version 1.1* (Apr. 16, 2018), https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11.

compliance with cybersecurity requirements, and incorporating suppliers into response and recovery planning.[20] Other bureaus in the Commerce Department, including the National Telecommunications and Information Administration (NTIA), the Bureau of Industry and Security (BIS), and the International Trade Administration (ITA) also bring to bear important market-oriented perspectives and legal authorities on these issues.

Additionally, legislation is pending in Congress that would impose statutory restrictions on certain suppliers. The U.S. House of Representatives recently overwhelmingly approved the National Defense Authorization Act (NDAA) for Fiscal Year 2019, which would prohibit federal procurement from companies that use certain named companies' equipment or services.[21] The Senate is considering similar legislation.[22]

The breadth and depth of Congressional and Executive Branch activities on supply chain issues underscores the importance of a coordinated Federal approach. While the FCC has a targeted role to play in ensuring the security and integrity of the communications network supply chain, that role should be carried out in concert with efforts already underway elsewhere across the Federal government. Piecemeal approaches by multiple agencies, each of which addresses only a portion of the issue, risk creating inconsistent policy implementation and overlapping or redundant regulatory burdens. Supply chain security policy should be administered in a holistic manner that coordinates SCRM efforts across all Federal agencies and all affected sectors would be the most effective means of addressing the issue. The Commission's proposal to address only equipment supplied for USF-supported networks and services represents just a small piece of a

---

[20] *Id.* at §§ 3.3, 3.4 and Table 1, ID:SC-1-ID:SC-5.

[21] National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Cong., at Div. A, § 880 (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.

[22] Defending U.S. Government Communications Act, S. 2391, 115th Cong. (2018).

larger and more complex issue that involves not only communications companies, but also IT suppliers, security vendors and tools specialists, cloud service providers, software suppliers and a range of other entities.

Therefore, the Commission should act only pursuant to statutory guidance from Congress or formal Administration guidance deriving from a DHS-led interagency process informed by input from relevant agencies and private sector stakeholders. If the Commission takes any action pursuant to this proceeding, it should ensure that such action complements and effectively advances the broader national and economic security objectives at stake here and aligns closely with supply chain initiatives that are being undertaken by other Federal agencies.

Promoting and Protecting Private Sector Stakeholder Input. The Commission also should assess the extent to which its own role in advancing those initiatives could be improved through further stakeholder input, particularly through the ongoing work of CSRIC and NIST. Given the Congressional preference expressed in the Cybersecurity Enhancement Act of 2014 for addressing cybersecurity issues via flexible and dynamic voluntary standards and industry-driven best practices,[23] the Commission should consider deferring action on the rules proposed in the NPRM pending progress on related activities at the FCC and elsewhere, including CSRIC's present work on supply chain security as well as the recently-begun DHS effort on Telecommunications Supply Chain Risk Assessments. This would also provide companies with more time to incorporate the SCRM guidance recently added to the NIST Cybersecurity Framework.

[23] *See* Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, § 101(a)-(b) (as codified in 15 U.S.C. § 272(c)(15)&(e)).

In the interest of government-industry engagement and mutually beneficial partnership in advancing cybersecurity, the Commission should look to CSRIC's past recommendations regarding Cybersecurity Risk Management and Best Practices.[24] Specifically, in order to create new avenues through which private sector companies could engage with the government in candid partnership without fear that such engagement will expose them to legal, regulatory, or business risks, CSRIC recommended that the FCC work with DHS to apply DHS's statutory confidentiality protections provided under the Protected Critical Infrastructure Information (PCII) program[25] to cybersecurity engagements between individual companies, the FCC and DHS. The PCII program was created by Congress for the express purpose of encouraging critical infrastructure owners and operators to share sensitive information with government entities.[26] The protections afforded by that program may provide the opportunity for a more targeted and less disruptive means of addressing risks and vulnerabilities in the communications network supply chain, with statutory protection of sensitive information provided by companies in these formal processes against public disclosure or in civil litigation and regulatory enforcement actions or rulemaking processes. The PCII protections are needed in this setting to provide for meaningful partnership between government and industry on the concerns that the Commission seeks to address in this proceeding. The Commission has issued a protective order for confidential information that companies may provide under this proceeding,[27] but it is

---

[24] *See* FCC – Communications Security Reliability and Interoperability Council, *Cybersecurity Risk Management and Best Practices - Working Group 4 Final Report*, at 6 (Mar. 2015), https://transition fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf (calling for "company-specific meetings" with the Commission and DHS under PCII protections).

[25] DEP'T OF HOMELAND SEC., *Protected Critical Infrastructure Information Program*, https://www.dhs.gov/pcii-program (last visited May 31, 2018).

[26] *See* 6 U.S.C. §§ 131 – 134; 6 C.F.R. §§ 29.1 – 29.9.

[27] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Protective Order, WC Docket No. 18-89, FCC 18-42 (rel. May 23, 2018).

insufficient for the partnership that is necessary here. Commission orders cannot provide the statutory protections against disclosure and use that PCII provides.

Conducting Analysis of Costs and Market Effects. The Commission also should assess the impact that restricting the ability of certain vendors to participate in telecommunications equipment markets would have on the costs of communications services, the deployment of advanced infrastructure, and the pace of innovation and product development. Changes to eligibility requirements for USF support based on supply chain concerns could impede those goals by significantly increasing equipment replacement and other costs and causing equipment availability disruptions as suppliers scramble to ensure compliance with new rules. Policy initiatives that effectively blacklist certain vendors also could affect the competitiveness and diversity of a network equipment marketplace already characterized by a relatively small number of suppliers. The Commission should carefully consider the marketplace effects of effectively shrinking the number of equipment vendors via supply chain regulatory constraints on USF support recipients prior to adopting any new rules.

III. ANY SUPPLY CHAIN RULES ADOPTED BY THE COMMISSION SHOULD PROVIDE USF RECIPIENTS CLARITY AND CERTAINTY REGARDING PERMITTED AND PROHIBITED VENDORS

To the extent the Commission elects to move forward with any proposed rules, it should provide clear guidance to providers to ensure regulatory certainty regarding the scope of the prohibition. Communications service providers need to have a clear understanding regarding the identity of blacklisted vendors and/or blacklisted vendor equipment to avoid uncertainty in buying decisions.

First, the Commission should clearly define the scope of its rules to avoid overbreadth and ensure that providers understand what is prohibited. For example, rather than impose a

blanket prohibition on the use of any equipment provided by a blacklisted vendor, the Commission should employ a more targeted approach. The NPRM notes that, in lieu of a prophylactic ban on all types of equipment from a blacklisted vendor, it instead might apply these rules only to equipment and services "that relate to the management of a network." The suggestion to narrow the scope of prohibition only to equipment that performs key network management functions is useful, but the NPRM does not define that concept or provide any guidance on what it might mean.[28] Modern network management is distributed across a variety of network elements. Moreover, cyber threat and attack points are dynamic and not limited to key network management components.

In lieu of defining "network management" functionality, the Commission should consider limiting the prohibition to a specific list of blacklisted equipment items that raise known and identifiable national security risks.[29] Alternatively, the Commission could cabin the scope of its prohibition to certain categories of equipment, such as equipment that performs core network routing or packet inspection functions – an approach reflected in some pending legislative proposals to limit Federal agencies from procuring certain equipment from Huawei or ZTE.[30]

Second, the Commission also should clarify that any restrictions would apply only if blacklisted network equipment is used in providing USF-supported services and would not be implicated simply because a communications provider used such equipment in connection with furnishing services outside the USF programs. If certain equipment is prohibited for use in

---

28 *Id.* ¶ 15.

29 *See id.*

30 *See, e.g.*, H.R. 5515, § 880(b)(4)-(5) (providing a process for excluding from agency procurement prohibition Huawei/ZTE equipment that does not perform routing or packet inspection functions); National Defense Authorization Act for Fiscal Year 2018, S. 1519, 115th Cong. (2018) (categorically excluding from agency procurement prohibition Huawei/ZTE equipment that does not perform routing or packet inspection functions).

providing a supported service pursuant to a USF program, that should not affect the ability of the equipment vendor or USF recipient to utilize such equipment outside the context of fulfilling its USF obligations. Prohibiting payments to *any* party using *any* covered equipment or services would risk causing widespread confusion and disruption and impose substantial administrative burdens on all parts of the USF ecosystem. The NPRM appropriately limits the proposed prohibition to the *use of USF funds* for covered equipment, and the Commission should reject any calls to convert the proposed ban into one that would prohibit the use of covered equipment by *any entity receiving USF funds*, as well as any entity that does not participate in the USF program which is being contracted and providing services to another provider which does participate in the USF program. Such an overbroad ban not only would constitute bad policy but also would exceed the Commission's authority under Section 254 of the Communications Act.

Third, any rules also should ensure that communications service providers receiving USF support are only responsible for what they can control. For example, if company A provides metro Ethernet to a school district via the E-rate program, and that school district proposes to purchase with its own money voice communications services from company B that uses equipment from a prohibited vendor, there should be no impact on company A. To the extent the Commission follows through on its suggestion to apply these rules to contractors and sub-contractors,[31] it also should consider adopting a safe harbor provision or scienter requirement protecting companies against being penalized due to the actions of a third party. While agreements with contractors and subcontractors could be modified to prohibit use of blacklisted equipment, ensuring compliance for all contractors and subcontractors would likely be difficult and burdensome. The Commission should consider establishing a safe harbor specifying that a

[31] *NPRM* ¶ 16.

USF recipient does not run afoul of any rules established in this proceeding if it prohibits use of blacklisted equipment/vendors in contracts and has a certification from contractors and subcontractors that they will not use equipment from prohibited companies.

Fourth, the NPRM states that any rules it adopts will have prospective effect only.[32] NCTA agrees that the Commission should not prohibit equipment that is already deployed and operational. Existing equipment from prohibited vendors should be grandfathered to avoid the disruptive effects of retroactive application. Applying any new blacklisting retroactively might well force premature retirement of equipment, especially as the blacklist evolves, which could adversely affect service provisioning and quality and increase network costs. For smaller entities, these increased costs could result in heightened need for additional USF support.

Even if the Commission appropriately opts to grandfather existing equipment, the NPRM also raises the possibility of the new rules constraining the patching and upgrading of already-deployed equipment.[33] If USF funds used for maintenance, software updates, and customer support fall within the scope of the proposed rules, that would either effectively mandate replacement of those products before the end of their life-cycle or force companies receiving USF monies to run outdated or inadequately maintained equipment. As a practical matter, this would penalize companies for equipment purchases they have already made, as well as penalize companies who have contracts with providers using already-deployed equipment for the length of their contracts, thereby imposing a retroactive effect and negating the relief associated with grandfathering. The Commission therefore should clarify that the use of USF funds to provide support for existing equipment is permitted, at least for some prescribed period that aligns with

---

[32] *Id*. ¶ 17 ("We make clear that our proposed rule or any alternative to restricting the use of USF funds that we adopt in the proceeding would apply only prospectively.").

[33] *Id*. ¶ 15 ("[W]e expect that the proposed rule would extend to upgrades of existing equipment or services.").

the useful life of such equipment. Otherwise, it would expand the scope of its proposal to include purchases made before the adoption of these rules.

Further, communications products and services are composed of a complex array of materials and equipment – e.g., chips, firmware, software, active and passive components and systems. This long supply chain necessarily involves manufacturers with multiple suppliers for the same materials used to assemble and build equipment for today's sophisticated networks. Given the long lead time associated with procuring communications network equipment, the Commission should provide for an interim transition period to adjust to any new supply constraints engendered by the rules.

Finally, in connection with any rules the Commission may adopt, it should ensure that its regulatory process adequately safeguards the critical, sensitive information at stake. This concern pertains not only to the highly sensitive business information concerning service providers' selection and use of particular network equipment, but also to industry participation in discussions with national security agencies as to foreign suppliers that might pose a security threat to the communications supply chain. As the federal government conducts intelligence assessments, it of course will have candid and forthcoming input from communications service providers, but the value of such input will depend on robust safeguards to protect the confidentiality of sources and information. The Commission should ensure that such confidentiality concerns remain paramount as it considers adopting rules addressing supply chain security.

IV. THE COMMISSION SHOULD BASE ANY ASSERTION OF AUTHORITY HERE TO ITS OVERSIGHT OF EXPENDITURES UNDER THE UNIVERSAL SERVICE FUND PROGRAM

The NPRM appropriately declines to ground the proposed rules in broad statutory language such as the reference to the "national defense" in Section 1 of the Communications Act.[34] Instead, the Commission looks specifically to its responsibility to administer the USF program as the basis for its assertion of authority here. The Commission notes that it has previously construed its authority under Section 254(b) granting it power to advance such objectives as quality service at reasonable rates, access to advanced telecommunications and other information services, and other principles necessary for protecting the public interest.[35] The NPRM states that "the promotion of national security is consistent with the public interest and hence USF funds should not be used to undermine national security."[36]

---

[34] *Cf. NPRM* ¶¶ 7, 35; *see also* FCC – Pub. Safety & Homeland Sec. Bureau, *White Paper - Cybersecurity Risk Reduction*, Appx. A at 33 (rel. Jan. 18, 2017) (citing Section 1 reference to "national defense" in the Communications Act as one of "FCC authorities for national security and cybersecurity"). In other contexts, Congress has explicitly directed other agencies to address supply chain. Supply chain-related legislation "includes the Security and Accountability for Every Port (SAFE Port) Act, the Maritime Transportation Security Act, the Aviation and Transportation Security Act, the Implementing Recommendations of the 9/11 Commission Act, and others." *See* DEP'T OF HOMELAND SEC., *National Strategy for Global Supply Chain Security*, at n.1 (Jan. 2013), https://www.dhs.gov/national-strategy-global-supply-chain-security. Federal agency supply chain issues are encompassed within the scope of NIST's responsibilities pursuant to the Federal Information Security Management Act (FISMA) of 2014. 44 U.S.C. § 3541; NAT'L INST. OF STANDARDS AND TECH., *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Special Publication 800-61, at ii (Apr. 2015) ("This publication has been developed by National Institute of Standards and Technology (NIST) in accordance with its statutory responsibilities under the Federal Information Security Modernization Act. . . . NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems."). Further, as the *NPRM* notes, specific restrictions on procurement of communications and information technology equipment by certain Federal agencies were enacted as part of the National Defense Authorization Act for Fiscal Year 2018. *See NPRM* ¶ 6. Congress also prescribed supply chain risk management practices for certain Federal agencies within this year's omnibus spending bill. *See* Consolidated Appropriations Act of 2018, H.R. 1625, 115th Cong., at Div. B, § 514 (imposing supply chain risk management guidelines and review procedures on Departments of Commerce, Justice, NASA, and the National Science Foundation).

[35] *NPRM* ¶ 35.

[36] *Id.*

As the NPRM implicitly recognizes, the Commission does not have plenary authority to regulate the communications network supply chain. Accordingly, the Commission should make clear that any rules adopted in this proceeding are simply funding conditions attendant to its congressionally delegated responsibility to administer the award of USF monies to recipients, rather than a reflection of plenary authority over private sector procurement decisions by communications companies.

CONCLUSION

For the foregoing reasons, NCTA urges the Commission to seek a holistic, well-coordinated interagency approach to securing and safeguarding the communications supply chain in the context of the Universal Service Fund program, in partnership with DHS, Commerce, and intelligence community initiatives addressing cybersecurity risks. The Commission also should undertake a cost-benefit analysis of any new rules to avoid potential adverse effects on communications network equipment pricing, competition, and innovation. And any USF supply chain rules should provide USF recipients with clarity and certainty on all aspects and the full scope of permitted and prohibited equipment and services.

Respectfully submitted,

/s/ Rick Chessen

Rick Chessen
Loretta Polk
NCTA- The Internet & Television Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431

June 1, 2018