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 CTIA

Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Thomas K. Sawanobori
Senior Vice President, Chief Technology Officer

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 Sixteenth Street, NW, Suite 600
Washington, DC 20036
(202) 736-3200

June 1, 2018

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 CTIA

CTIA[1] respectfully submits these comments in response to the Federal Communications Commission's (Commission) Notice of Proposed Rulemaking (NPRM), *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*.[2]

I. INTRODUCTION AND SUMMARY

CTIA and its member companies view the security of the U.S. communications sector's supply chain as a fundamental necessity of reliable mobile wireless communications, and we share the Commission's commitment to protecting these critical services from malicious actors. Wireless networks are designed and operated with numerous built-in protections to minimize the opportunities for bad actors to compromise the integrity of networks and wireless communications. As a result of the wireless industry's collective and ongoing efforts and

[1] 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, and 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*, Notice of Proposed Rulemaking, WC Docket No. 18-89, FCC 18-42 (rel. Apr. 18, 2018).

engagement on issues of security, each new generation of wireless technology is more secure than the last.

Given the multi-faceted and interdependent components of mobile wireless communications networks, securing the U.S. communications sector's supply chain must be a well-coordinated partnership between the federal government agencies with appropriate jurisdiction and communications industry stakeholders. In particular, while this proceeding may demonstrate how the Commission might implement supply chain security measures through its universal service programs, efforts to secure the U.S. communications sector's supply chain should be led by the U.S. Department of Homeland Security (DHS) as the Sector Specific Agency for both the communications and IT sectors. Thus, the Commission's efforts in this proceeding should be consistent with the U.S. government's broader efforts on these issues.

The global supply chains for hardware, software, and related services that fuel the innovation throughout the evolving U.S. communications sector are diverse and multi-national. For this reason, even Commission action in this proceeding that would be narrowly focused on universal service programs could impact exceptionally multifaceted and complex geopolitical and global economic issues. Relatedly, international, diplomatic, and global economic dynamics also have a major impact on the evolving threat landscape within the U.S. communications sector. For this reason, the Commission should proceed with care to ensure that its rules do not constrain the ability of the U.S. communications industry to react in real time to changing circumstances.

In particular, given the multiple ongoing information and communications technology (ICT) supply chain initiatives being undertaken throughout the federal government, Commission action in this proceeding should provide sufficient flexibility for affected entities to

accommodate other related government efforts or requirements. In order to maximize the effectiveness of security efforts, industry stakeholders need consistent policies and navigable processes across the federal government. Likewise, the Commission should ensure that any action in this proceeding sets a floor, and not a ceiling, on affected entities' ability to adapt to an evolving cybersecurity threat environment.

Further, the proposed rules would have broad implications for wireless carriers participating in the Commission's Universal Service Fund (USF) programs and their customers – with respect to, for example, security, innovation, and investment, among others. If pursued, the Commission's rules for the universal service programs should be designed to maximize clarity, predictability, and efficiency.

II. THE WIRELESS INDUSTRY WORKS TO PROACTIVELY ANTICIPATE AND RESPOND TO SUPPLY CHAIN SECURITY RISKS AND WORKS DILIGENTLY TO PROTECT ITS NETWORKS, DEVICES, AND CONSUMERS AGAINST EVOLVING GLOBAL SECURITY THREATS

The Commission's consideration of these issues should start from the premise that the wireless industry is deeply engaged in cybersecurity efforts in general and supply chain security in particular. Indeed, for its part, the wireless industry is on the front lines every day protecting consumers, networks, and technology from security threats.

Wireless networks are designed and operated with numerous built-in protections to minimize the opportunities for bad actors to compromise the integrity of networks and wireless communications.[3] For example, the wireless industry has developed air interfaces with standards-based encryption to safeguard wireless communications in transit, as well as

[3] *See* CTIA, *Protecting America's Wireless Networks*, Apr. 2017, https://api.ctia.org/docs/default-source/default-document-library/protecting-americas-wireless-networks.pdf.

authentication standards for devices and users on networks, using enhanced cryptographic keys to validate and authorize access to the network. Ciphering and coding data travels over wireless networks to ensure that the networks remain free from corruption and unauthorized modification, and strict access controls are in place to limit and monitor physical and virtual network access. Wireless networks are built with multiple redundancies and other robust network management practices that increase the availability and reliability of the networks.

In addition to network security measures, the wireless industry has worked to ensure that mobile devices have incorporated significant security protections to protect against an evolving threat environment. These include the integration of Subscriber Identification Module (SIM) cards that securely store data and ensure appropriate network authentication, use of temporary credentials that vary regularly to minimize risks of unauthorized use or interception, and the use of hardware-based roots-of-trust cryptographic information to detect malware and authenticate system software integrity. Furthermore, mobile operating system developers and app marketplace operators also work diligently to create a device operating environment free of malware, viruses, and other threats.

The wireless industry collaborates to address emerging and evolving threats of all kinds, sharing information and best practices domestically and abroad about risks and mitigations. Wireless industry members are active participants in standard setting bodies, including ATIS, 3GPP, and IETF, which strive to develop, update, and maintain global standards to ensure the security and integrity of the mobile communications ecosystem. The industry also focuses on consumer outreach and education to ensure that consumers are able to take control of their own

security while also understanding limitations.[4] Industry research shows that consumer education about security best practices can be quite effective.[5]

As a result of the industry's ongoing efforts and engagement on issues of security, each new generation of wireless technology is more secure than the last. Both second and third generations of mobile service provided for network-based authentication of mobile devices as well as data encryption capabilities, and added authentication and encryption that deterred eavesdropping and fraudulent service theft. Fourth generation wireless technology offered a stronger security platform, involving an end-to-end security architecture with strong cryptographic and authentication techniques to ensure a secure environment. Fifth generation technology will be even more secure, featuring encryption of International Mobile Subscriber Identity (IMSI), improved home network control of authentication, and authentication of WiFi in addition to cellular connections.

The wireless industry has a close and longstanding partnership with DHS, involving both information sharing and operational coordination. The industry collaborates with the DHS National Coordinating Center for Communications (NCC), the Communications Information Sharing and Analysis Center (Comm ISAC), and the Communications Sector Coordinating Council (CSCC) on a wide variety of cyber and physical threats, national level exercises, natural disasters, emergency response, and national security events. Several industry members also

---

[4] *See* Comments of CTIA, *Public Safety and Homeland Security Bureau Requests Comment on Implementation of Signaling System 7 Security Best Practices*, PS Docket No. 18-99, at 15-16 (filed May 3, 2018).

[5] For example, a CTIA-commissioned Harris Poll conducted in 2016 found that 69 percent of wireless consumers use PINs/passwords on their smartphones, up 13 percent from 2015 and up 38 percent from 2012, while 51 percent of consumers have built-in remote lock and erase software installed on their smartphones, up 42 percent from 2015 and up 31 percent from 2012. *See* CTIA, *Survey Shows Americans Follow Wireless Companies' Consumer Education Efforts on Mobile Security*, July 21, 2016, https://www.ctia.org/news/survey-mobile-security.

participate on the National Security Telecommunications Advisory Council (NSTAC), which provides strategic policy advice to the President on National Security and Emergency Preparedness (NS/EP) communications and other communications reliability and cybersecurity matters. These partnerships with government actors have produced concrete benefits for consumers and demonstrable advancements for security, ranging from coordinated responses to cyber attacks such as the Dyn IoT DDoS, as well as natural disasters, to "Cyber Storm" exercises conducted with government partners that yielded important lessons for improved incident response going forward.[6]

CTIA, for its part, also facilitates regular engagement with DHS through its Cybersecurity Working Group, where NCC representatives are regular attendees at meetings hosted by CTIA with industry subject-matter-experts to address ongoing collaboration regarding mobile cybersecurity.

The partnership represented by all of the above activities is particularly important in connection with the specific security concerns underlying the NPRM. As the report recently prepared for the U.S.-China Economic and Security Review Commission highlighted, defending against nefarious action by Chinese companies "requires communication and collaboration with private sector actors."[7] The wireless industry therefore approaches this proceeding with the same strong commitment to security that it has exhibited for many years. In considering its next steps

[6] *See* Department of Homeland Security, *Cyber Storm: Securing Cyber Space*, https://www.dhs.gov/cyber-storm.

[7] Interos Solutions, Inc., *Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology*, at vi (Apr. 2018) ("Report for U.S.-China Security Review Commission"), https://www.uscc.gov/Research/supply-chain-vulnerabilities-china-us-federal-information-and-communications-technology.

in this proceeding, the Commission should build on these significant ongoing efforts while also proceeding with caution so as to avoid disruption to existing processes for mobile cybersecurity.

III. COMMISSION ACTION MUST BE CONSISTENT WITH BROADER U.S. GOVERNMENT EFFORTS ON COMMUNICATIONS SUPPLY CHAIN SECURITY, LED BY DHS AS THE SECTOR SPECIFIC AGENCY FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY

On a variety of fronts, Executive Branch agencies and departments with security expertise, as well as Congress, are concurrently pursuing solutions to the same concerns highlighted in the NPRM – including by taking the necessary first step (outside of the Commission's own expertise) of identifying which companies pose the greatest national security risks. These ongoing initiatives, together with the constant evolution of U.S. international trade and investment policy, contribute to the highly fluid environment that the Commission entered with its commencement of this proceeding. The Commission thus should endeavor through any action it takes in this proceeding to help advance a well-coordinated approach across the federal government that deepens public-private cooperation to develop and implement solutions to these challenges.

A. Other Federal Agencies and Departments Are Actively Assessing and Responding to National Security Threats Posed by Certain Suppliers.

As will be discussed in greater detail below, there is an abundance of work and examination ongoing throughout the federal government on supply chain security.

1. DHS, As the Sector Specific Agency for Communications and IT, Should Lead on Communications Supply Chain Security Issues.

Of the various government actors active in this area, the Commission should remain particularly cognizant of the role and capabilities of DHS, the Sector Specific Agency for both the communications and IT sectors. Historically, the U.S. approach to cybersecurity and national security in the communications sector has been built on partnerships and collaboration with DHS

and its predecessor components. DHS is well-positioned to lead further efforts in this space because of its expertise, its access to classified intelligence information, and its ability to protect the confidentiality of sensitive information shared by the private sector.[8] DHS has been actively engaged on supply chain issues for government and the private sector. The agency's Binding Operational Directives (BODs) for government networks are closely watched outside the government.[9] Further, DHS's recently announced initiatives to conduct general and targeted supply chain security risk assessments in the communications sector are an important new step that – if coordinated with other relevant agencies and conducted with proper protections for industry participants that share sensitive information – could serve as a foundation for broader interagency supply chain security efforts that reach other sectors.[10]

DHS's work in protecting the supply chain reflects the approach of an Administration that has made network security and protection of critical infrastructure a high priority. The Administration's National Security Strategy (NSS) seeks to protect and promote the "U.S. National Security Innovation Base," and states that "[s]upport for a vibrant domestic manufacturing sector, a solid defense industrial base, and resilient supply chains is a national

---

[8] *See* discussion of Protected Critical Infrastructure Information protections, *infra* Section IV.C.

[9] *See, e.g.*, Department of Homeland Security, *DHS Statement on the Issuance of Binding Operational Directive 17-01* (Sept. 13, 2017), https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01 (ordering agencies to "identify any use or presence of Kaspersky products on their information systems in the next 30 days, to develop detailed plans to remove and discontinue present and future use of the products in the next 60 days, and at 90 days from the date of this directive, unless directed otherwise by DHS based on new information, to begin to implement the agency plans to discontinue use and remove the products from information systems").

[10] *See* Lauren Williams, *DHS developing supply chain security initiative*, FCW, Feb. 14, 2018, https://fcw.com/articles/2018/02/14/dhs-supply-chain-security.aspx ("The Department of Homeland Security launched an internal supply chain cybersecurity initiative to determine where government agencies and private companies are lacking, the agency's top cyber official Jeanette Manfra announced at a Brookings Institution tech event in Washington, D.C., Feb. 14.").

priority."[11] The NSS also provides that the Administration will "work with the Congress to strengthen the Committee on Foreign Investment in the United States (CFIUS) to ensure it addresses current and future national security risks."[12]

2. The Commission's Actions Should Be Consistent with Other Agencies Throughout the Government That Are Also Focusing on Communications Supply Chain Issues.

There are multiple pertinent workstreams underway in the Executive Branch on these issues. For instance, in May 2017, the Administration issued an Executive Order requiring agencies to address ways to collaborate with industry to protect critical infrastructure and strengthen the deterrence posture of the U.S., among other requirements.[13] In support of this Executive Order, the Executive Office of the President asked the NSTAC to "examine how the private sector and government could improve the resilience of the Internet and communications ecosystem" and "identify ways to encourage collaboration to reduce the threats from automated and distributed attacks." Among many other recommendations, the resulting NSTAC Report called for supply chain scrutiny and simplification of "several overlapping efforts to improve

[11] *See* National Security Strategy of the United States of America, at 30 (Dec. 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[12] *Id*. at 22. CFIUS has been actively blocking Chinese transactions involving critical infrastructure. The new CFIUS reform bill, the Foreign Investment Risk Review Modernization Act of 2017 (FIRRMA), would, as currently drafted, significantly impact Chinese investment and U.S. joint ventures with Chinese entities in the U.S. and abroad. Further, it would give CFIUS the power to review IP transfers that involve the provision of services and require mandatory declarations for investments by government controlled entities. *See* H.R. 4311, 115th Cong. (2017-2018), https://www.congress.gov/bill/115th-congress/house-bill/4311.

[13] *See* Executive Order 13800, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

supply chain security from a variety of agencies including NIST (the National Institute of Standards and Technology), DHS, and the FCC."[14]

NIST is broadly recognized as being particularly "effective in partnering with the private sector to produce high-quality, implementable standards to improve supply chain security and cybersecurity of ICT systems, including the widely adopted NIST Cybersecurity Framework."[15] In fact, the newest revision of the NIST Cybersecurity Framework includes new guidance for supply chain risk management and provides companies tools and actionable best practices for reducing risk.[16] Beyond the NIST Cybersecurity Framework, NIST has published guidance on Supply Chain Risk Management for federal agencies, which many private companies use, and has also evaluated several examples of cyber supply chain risk management.[17]

Other agencies within the Executive Branch are also active in support of the Administration's focus on securing the ICT supply chains for critical infrastructure, acting within their respective legal responsibilities to highlight and mitigate concerns about the companies named in the NPRM and making clear that the Administration is committed to addressing threats across the economy. For instance, the Office of the U.S. Trade Representative recently issued a report citing "evidence … that China continues its policy and practice, spanning more than a

---

[14] The President's National Security Telecommunications Advisory Committee, *NSTAC Report to the President on Internet and Communications Resilience*, at 35 (Nov. 16, 2017), https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20%2810-12-17%29%20%281%29-%20508%20compliant_0.pdf.

[15] *See, e.g.*, Report for U.S.-China Security Review Commission at vi.

[16] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (Apr. 16, 2018) ("NIST Cybersecurity Framework"), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[17] National Institute of Standards and Technology, *Cyber Supply Chain Risk Management, Industry Best Practices For Cyber SCRM*, https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management/Best-Practices.

decade, of conducting and supporting cyber-enabled theft and intrusions into the commercial networks of U.S. companies,"[18] and subsequently proposed to implement tariffs on a number of Chinese goods.[19] Additionally, the Department of Commerce's recent action banning U.S. exports to ZTE due to violations of U.S. export controls law underscores that the Administration's concerns about these companies extend beyond the supply chain security context.[20] At the same time, that episode vividly illustrates how rapidly the policy environment can change, as more recent reports indicate that the Administration is considering mitigating the impact of the Department of Commerce's penalties on ZTE as part of broader negotiations pertaining to trade and national security considerations.[21]

The Department of Justice (DOJ) and the Department of Defense (DOD), of course, also have roles to play in connection with protecting the security of the nation's critical infrastructure. For instance, DOJ recently created a Cybersecurity Task Force to canvass the many ways that DOJ is combatting the global cyber threat, including threats to the ICT supply chain, and to

---

[18] *See* Office of the United States Trade Representative, Executive Office of the President, *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974*, at 154 (Mar. 22, 2018), https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

[19] Office of the United States Trade Representative, *Notice of Determination and Request for Public Comment Concerning Proposed Determination of Action Pursuant to Section 301: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation*, 83 Fed. Reg. 14,906 (Apr. 6, 2018), https://www.gpo.gov/fdsys/pkg/FR-2018-04-06/pdf/2018-07119.pdf.

[20] *See* U.S. Department of Commerce, Bureau of Industry and Security, *Zhongxing Telecommunications Equipment Corporation and ZTE Kangxun Telecommunications Ltd., Order Activating Suspended Denial Order Relating to Zhongxing Telecommunications Equipment Corporation and ZTE Kangxun Telecommunications Ltd.* (Apr. 15, 2018) ("*ZTE Export Denial Order*"), https://www.commerce.gov/sites/commerce.gov/files/zte_denial_order.pdf. The sector is working with the Department of Commerce on implementation and transition challenges, further demonstrating the complexity of supply chain issues.

[21] Ana Swanson, *Trump Administration Plans to Revive ZTE, Prompting Backlash*, N.Y. TIMES, May 25, 2018, https://www.nytimes.com/2018/05/25/us/politics/trump-trade-zte.html.

identify how federal law enforcement can more effectively accomplish its mission.[22] In December, DOJ entered into an agreement with Netcracker Technology Corp. wherein Netcracker agreed to implement enhanced security protocols for software development, implementation and other services to clients, many of whom are part of the country's critical communications infrastructure.[23] DOD has long undertaken steps to secure the ICT supply chain for its own networks and for those of the companies that make up the Defense Industrial Base.[24] Most pertinent to this proceeding, DOD is subject to legislation enacted late last year that prohibits Huawei and ZTE from being used in certain DOD networks,[25] and in early May, DOD announced a new policy banning sales of Huawei and ZTE mobile handsets at stores on military bases worldwide.[26]

In short, the Commission should remain cognizant of the fact that the challenge of securing the U.S. communications sector is shared among various government stakeholders – many of which have already identified specific security concerns and crafted specific solutions to

---

[22] *See* Department of Justice, *Attorney General Sessions Announces New Cybersecurity Task Force*, Press Release 18-196, Feb. 20, 2018, https://www.justice.gov/opa/pr/attorney-general-sessions-announces-new-cybersecurity-task-force.

[23] *See* Department of Justice, *National Security Division Announces Agreement with Netcracker for Enhanced Security Protocols in Software Development*, Press Release 17-1394, Dec. 11, 2017, https://www.justice.gov/opa/pr/national-security-division-announces-agreement-netcracker-enhanced-security-protocols.

[24] *See* Department of Defense, *Defense Industrial Base, Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan*, May 2007, https://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base.pdf.

[25] National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, div. A, § 1656, 131 Stat. 1283, 1762 (Dec. 12, 2017), *available at* https://www.congress.gov/115/bills/hr2810/BILLS-115hr2810enr.pdf (enrolled bill).

[26] *See, e.g.*, Hamza Shaban, *Pentagon tells U.S. military bases to stop selling ZTE, Huawei phones*, WASH. POST, May 2, 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/05/02/pentagon-tells-u-s-military-bases-to-stop-selling-zte-huawei-phones/?utm_term=.634b70fc3dfe.

address them. As the Commission is not well-positioned to determine which suppliers could most readily put that security at risk,[27] the Commission should ensure that any actions in this proceeding are consistent and do not conflict with actions of other agencies.

B. Any Commission Action Should Be Consistent with Related Legislative Initiatives.

As the Commission begins to consider targeted actions it can take within its authority to address supply chain concerns, Congress is also pursuing significant legislation that would impose broader statutory restrictions on the suppliers identified in the NPRM and potentially additional companies. While the NPRM notes some of this activity,[28] the situation remains sufficiently fluid that the full extent of legislative outcomes is still unclear, thus warranting careful attention by the Commission as it works through the proposals and arguments made in this proceeding.

To note the most prominent example, last week the House of Representatives overwhelmingly approved the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019, which, as with companion legislation in the Senate, would prohibit *all* federal procurement from Huawei and ZTE and companies that use Huawei and ZTE equipment or services.[29] In

---

[27] *See, e.g.*, discussion of Protected Critical Infrastructure Information protections, *infra* Section IV.C

[28] NPRM ¶¶ 4-6.

[29] National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Cong., div. A, § 880 (as passed in House on May 24, 2018 by a recorded vote of 351-66) ("H.R. 5515, § 880"), 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). Specifically, this proposal, contained in Section 880 of the FY19 NDAA, would ban agencies from working with "an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system" and names as covered equipment that from Huawei or ZTE, services provided using such equipment, or "an

doing so, this proposed legislation would continue a practice dating to at least 2011 of using the NDAA process to address specific concerns about the suppliers named in the NPRM.[30] On May 23, prior to passage of the full NDAA, the House of Representatives approved amendments to this bill that named three additional Chinese video surveillance companies as prohibited suppliers.[31] As the Senate considers similar legislation and as the NDAA moves toward likely enactment of some form of this provision later this year, the Commission should take care to ensure that any action it takes will complement any new statutory environment.

IV. THE COMMISSION'S TARGETED ROLE SHOULD AIM TO ADVANCE BROADER GOVERNMENT EFFORTS TO ENSURE SUPPLY CHAIN SECURITY

As discussed above, multiple efforts are underway throughout the federal government to address supply chain security concerns. In order for these efforts to have the intended effect, they must be coordinated amongst all relevant agencies and industry partners and focus on those

---

entity that the head of the relevant agency reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country."

[30] For instance, the report from the House Armed Services Committee on the NDAA for FY 2012 cited "the potential ties between the Chinese Government and malicious actors within China," and went on to note the committee's "alarm[] that two state-owned Chinese firms, Huawei and ZTE, have been included on the Department of Agriculture's list of safe and approved telecommunications equipment providers for the U.S. broadband expansion program" and its "concern[] about the potential threat this may pose to national security as well as to Department of Defense data." H.R. Rep. No. 112-78, at 198 (2011), https://www.congress.gov/112/crpt/hrpt78/CRPT-112hrpt78.pdf; *see also* NPRM ¶ 6 (noting that the NDAA for FY2018 bars DOD from using equipment and services provided by Huawei and ZTE for certain critical programs, and bars all federal agencies, including the Commission, from using any products or services made in whole or in part by Kaspersky Lab).

[31] 164 Cong. Rec. H4606-H4673 (daily ed. May 23, 2018) (voice vote agreeing to H. Amdt. 645 offered by Rep. Mac Thornberry to H.R. 5515, 115th Cong.), https://www.congress.gov/amendment/115th-congress/house-amendment/645/text; *see also* Dan Strumpf, *Bill Moves to Block U.S. From Buying Chinese Surveillance Equipment*, WALL ST. J., May 25, 2018, https://www.wsj.com/articles/bill-moves-to-block-u-s-from-buying-chinese-surveillance-equipment-1527239988.

portions of the supply chain that pose the greatest risk. As the Commission considers next steps, it should be cognizant of these other actions and take full advantage of available resources and protections available.

A. The Commission Must Coordinate with Other Agencies, and Also Draw on CSRIC's Expertise.

The Commission's action here will be the first such rulemaking in the communications or IT sectors, and it may set a precedent among other government agencies – or even a future Commission – for further supply chain requirements outside the universal service setting. Unilateral Commission action that is not coordinated with parallel efforts in other parts of the government could prompt other independent regulators to go their own way in regulating supply chain security. In worst case, this could lead to different or even conflicting requirements for different sectors of the economy.

Therefore, the Commission should proceed carefully and in coordination with other government and industry partners. The Commission has been involved in supply chain security issues prior to adopting the NPRM, but only through the diverse industry expertise the Commission convenes for its Communications Security, Reliability, and Interoperability Council (CSRIC). Indeed, the present CSRIC has been looking at supply chain security in connection with its assigned task to identify "(ii) mechanisms to best design and deploy 5G networks to mitigate risks to network reliability and security posed by the proliferation of Internet of Things devices, vulnerable supply chains, and open-source software platforms used in 5G networks."[32] This present work follows previous CSRIC supply chain security studies, including a focus on

[32] *See* CSRIC VI Working Group Descriptions, at 3 (Mar. 14, 2018), https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2018/mar/cs2018_0095.pdf.

hardware and software "security by design" in 2016.[33] In March 2015, CSRIC released its groundbreaking report on Cybersecurity Risk Management and Best Practices, calling for "confidential company-specific meetings" with the Commission and DHS, under the statutory Protected Critical Infrastructure Information (PCII) confidentiality protections.[34] More broadly, CSRIC's efforts over the past several years have forged a productive relationship between the Commission and industry, with valuable input by DHS, and thus provide an important foundation for this proceeding – and also for broader interagency efforts that this proceeding should endeavor to complement.

B. Any Commission Action Should Advance the Government's Examination of Which Portions of the ICT Ecosystem Pose the Most Risk.

Pursuant to CSRIC's ongoing work and building on its previous risk management recommendations, the Commission should focus its initial action in this proceeding on determining the types of equipment that pose the most risk. Determining where to draw these lines, particularly in a setting in which the government is concerned about nation-state-based threats leveraging certain suppliers, is itself a highly complex question that deserves diverse input from industry and government stakeholders, fosters collaboration, and provides adequate confidentiality protections. For example, a security compromise that a nation-state intelligence service may have embedded in a certain supplier's core network equipment could have broad

[33] *See* CSRIC V, *Secure Hardware and Software: Security-By-Design, Voluntary Security-by-Design Attestation Framework for Hardware and Software Critical to the Security of the Core Communications Networ*k, Working Group 6 Final Report, at A-6 (Sept. 2016), https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG6_Final_091416.docx (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).

[34] *See* CSRIC IV, *Cybersecurity Risk Management and Best Practices, CSRIC IV, Working Group 4: Final Report*, at 6 (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

implications for all users of that network – indeed, for the reliability of the network itself – whereas a similar security compromise to that supplier's line of mobile smartphone handsets constitutes a threat that is more targeted to the security of the communications of the individuals using those particular devices.

Ascertaining the differing levels of risk and the various industry and government approaches that may be best to address those differing risks is not well-suited for prescriptive regulations from a single independent agency; instead, decisions about supply chain risks should be made through a process coordinated by DHS that includes the many other agencies that regularly balance the competing equities and sensitive intelligence, as well as the diplomatic consequences of designations as other countries react to U.S. government action. While the Commission is not well-positioned to identify companies posing a national security risk independently of a broader interagency process, its input into such a process could include weighing in on the particular aspects of the communications ecosystem and related network considerations on which it has unique expertise.[35]

Moreover, because the Commission's legal authority on these issues – particularly beyond placing conditions on USF support – is unclear, Commission action to impose obligations related to supply chain security risk management may lead to uncertainty from the changing perspectives regarding regulatory jurisdiction that often comes with Commission leadership changes. Developing a holistic government approach to supply chain security issues requires legal certainty that cannot be provided by the Commission alone given the legal

[35] Similarly, just as the Commission should not act unilaterally to lead on critical infrastructure and national security issues, and should derive its supply chain determinations from these broader DHS-led processes, CTIA believes the Commission's existing role on equipment and device approvals should remain clear and unchanged. Neither DHS nor any other agency should intrude on the Commission's long-established role on equipment and device approvals.

uncertainties that attend its proper role and authorities on these issues. Therefore, for long-term planning and procurement processes, buyers of equipment and services need certainty about trusted suppliers through processes based on broader authority and perspectives than those the Commission possesses alone.

In short, any action the Commission takes in this proceeding should complement and help advance – not conflict with, preempt, or unduly influence – broader governmental efforts to ensure the security of the U.S. critical infrastructure ICT supply chain. With that in mind, the Commission should allow for flexibility to accommodate or adapt to any changes and insights that arise from these broader processes. As discussed in detail above,[36] in recent months alone, there have been multiple government actions or initiatives on these issues, many of which are still ongoing. These various efforts must be integrated into a well-coordinated and coherent whole-of-government effort. The Commission can play an important, but consultative, role on these issues, but it should coordinate any actions it takes in this proceeding with other important players in the federal interagency process, and in no circumstances should the Commission or any other regulator make its own national security determinations on this issue.

C. Given the Sensitivities of This Information, PCII Protections Are Needed.

This proceeding should help develop mechanisms for fulsome input from a diverse range of government agencies and private sector stakeholders with interests in supply chain security. As mentioned above, government-industry discussions about supply chain security and network equipment – particularly regarding the specific nation-state threats that have given rise to this NPRM – are not well-suited for public notice and comment proceedings. On this topic, CTIA reiterates CSRIC's 2015 recommendation that private sector input to the government on such

[36] *See supra* Section III.

critical and sensitive topics should be afforded statutory PCII protections, administered by DHS, to guarantee that sensitive information industry discloses to the government in connection with cybersecurity risk management will not be publicly disclosed (under the Freedom of Information Act or similar State, local, tribal, or territorial disclosure laws) and will not be used in civil litigation or for regulatory enforcement actions or rulemaking proceedings. Although the Commission has released a protective order to govern the submission and review of confidential information in this proceeding,[37] that step is not sufficient to address confidentiality concerns, as a Commission-issued protective order cannot provide protections that carry the certainty that statutory PCII protections provide.

V. IF PURSUED, ANY IMPLEMENTATION WITHIN USF SHOULD MAXIMIZE CLARITY AND EFFICIENCY WHILE MINIMIZING DISRUPTION FOR RECIPIENTS

To the extent the Commission imposes a condition that USF support not be used on products from suppliers deemed to pose national security threats, it should provide clear guidance to the Universal Service Administrative Company (USAC) regarding its role in implementing, overseeing, and enforcing any restrictions or prohibitions that arise from this proceeding. USAC should not have any national security- or supply chain-based discretion in delivering, evaluating, or auditing the use of USF by recipients beyond executing the direction provided through the Commission. In this and all other facets of implementation of prohibitions or restrictions within USF, any Commission rule, restriction, or prohibition arising from this proceeding should provide USAC and USF recipients clear guidance.

[37] *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).

The NPRM's stated intent to apply this rule only prospectively begs a number of questions that should be answered in favor of maximizing efficiency and minimizing disruption to federal USF recipients following adoption of a rule and imposition of any restrictions or prohibitions. The Commission should further clarify what impacts a prospective rule has on existing equipment and relationships.[38] To the extent the Commission imposes supply chain risk conditions upon receiving federal USF support, it should create clear and navigable processes for USF recipients who have potentially-prohibited/restricted equipment that was purchased prior to its designation as prohibited/restricted to receive continued USF support, even though reasonable upgrades and maintenance service for that equipment may require continued transactions with the potentially-prohibited/restricted vendor.

The Commission should also consider whether to provide reasonable periods for phase-in of the prohibitions or restrictions as well as meaningful processes to seek waivers for exigent circumstances. Notably, the pending FY 2019 NDAA provisions banning Huawei and ZTE from government and government contractor networks would go into effect in 2021, and provide for a time-limited waiver beyond that time.[39] The Commission should consider whether similar timing is appropriate here and how any possible restrictions arising out of this proceeding would align with timing and implementation of such statutory requirements.

VI. CONCLUSION

For the foregoing reasons, CTIA encourages the Commission to work cooperatively and in close coordination with DHS, other government counterparts, and private sector stakeholders

[38] *See, e.g.*, *ZTE Export Denial Order* at 12-14, which prohibits entities from engaging in any transaction to service any commodity, software, or technology exported from the U.S. that is owned, possessed, or controlled by ZTE. The *ZTE Export Denial Order* defines "servicing" as "installation, maintenance, report, modification or testing." *Id*. at 14.

[39] *See* H.R. 5515, § 880.

in any action it may take in this proceeding to secure the U.S. communications sector's supply chain. The Commission's actions should be targeted to its unique role in overseeing and administering federal universal service funds. Cooperation and coordination across the federal government is necessary to ensure that the FCC's action complements other, related government initiatives, and also that it facilitates industry's ongoing response to a highly fluid policy and threat environment. Finally, the Commission should defer determinations about which companies pose a national security risk to DHS and other agencies with the requisite national security expertise. CTIA and the wireless industry will continue to maintain their active collaboration with the Commission, DHS, and other government partners, and the communications sector more generally to achieve these critical objectives.

Respectfully submitted,

/s/ Melanie K. Tiano

Melanie K. Tiano
Director, Cybersecurity and Privacy

Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Thomas K. Sawanobori
Senior Vice President, Chief Technology Officer

CTIA
1400 Sixteenth Street, NW, Suite 600
Washington, DC 20036
(202) 785-0081

June 1, 2018