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

In the Matter of Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program	ET Docket No. 21-232

COMMENTS OF 5G AMERICAS

Chris Pearson

5G AMERICAS
1750 112th Avenue NE
Bellevue, WA 98004

President of 5G Americas

September 20, 2021

TABLE OF CONTENTS

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

In the Matter of Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program	ET Docket No. 21-232

COMMENTS OF 5G AMERICAS

5G Americas, the voice for 5G and LTE in the Americas, submits these comments in response to the Commission's Notice of Proposed Rulemaking ("*Notice*" or "*NPRM*") and Notice of Inquiry ("*NOI*") in the above-referenced proceeding on protecting the communications supply chain through its equipment authorization authority.[1] Currently chaired by AT&T, 5G Americas has a broad membership of leading wireless operators and vendors of 5G core and radio access network equipment and software. 5G Americas facilitates and advocates for the advancement and transformation of LTE, 5G and beyond throughout the Americas.[2]

[1] *Protecting Against National Security Threats to the Communications Supply Chain*, Notice of Proposed Rulemaking and Notice of Inquiry, FCC No. 21-73, ET Docket Nos. 21-232, 21-233 (Rel. Jun. 17, 2021) ("*Protecting Against National Security Threats*"). 5G Americas comments directed to proposals in the NPRM can be found on pages 2-3 and our comments directed to questions in the NOI may be found on pages 4-12.

[2] 5G Americas Board of Governors include AT&T, Cable & Wireless Communications, Ciena, Cisco, Crown Castle, Ericsson, Intel, Mavenir, Nokia, Qualcomm, Samsung, Shaw, T-Mobile USA, VMware, WOM, and Telefónica. *Board of Governors,* 5G Americas, https://www.5gamericas.org/about/board-of-governors/.

INTRODUCTION AND SUMMARY

5G Americas shares the Commission's goal of advancing the security of equipment deployed in U.S. networks, but cautions the Commission not to make the application of its regulations retroactive, nor duplicate efforts of other agencies relative to ensuring IoT device security assurance including software cybersecurity. The Commission has important authority under the Communications Act and recent legislation that provide it ample ways to help secure the communications supply chain without subjecting industry to multiple cybersecurity and software compliance regimes or establishing the dangerous precedent of rescinding existing equipment authorizations. The Commission can receive technical recommendations on cybersecurity best practices from its advisory council, the Communications Reliability, Security and Interoperability Council ("CSRIC VIII"), recently revitalized under Acting Chairwoman Rosenworcel's leadership to include important federal partners.[3] 5G Americas suggests that the Commission seek CSRIC VIII's input on how to most effectively secure the communications supply chain.

I. THE NPRM DOES NOT JUSTIFY RETROACTIVE RESCISSION OF EQUIPMENT AUTHORITY

5G Americas appreciates the Commission's exploration of all avenues to help secure U.S. networks from untrustworthy equipment, but we do not support retroactive rescission of equipment authorization previously granted by the Commission under these circumstances either directly or through delegation to a recognized Telecommunications Certification Body.[4] The Commission

[3] *See Acting Chairwoman Jessica Rosenworcel Announces Member of Revitalized Communications Security, Reliability And Interoperability Council* (September 14, 2021), available at https://www.fcc.gov/document/fcc-announces-csric-viii-members-sept-22-meeting

[4] It is not the position of 5G Americas that the revocation of equipment authorizations would never be appropriate, but rather the circumstances set forth in the NPRM do not warrant that recourse. The rule (47 CFR 2.939(a)) regarding revocation of equipment authorization could be appropriate to invoke, for example, where cases of harmful interference are discovered.

seeks comment[5] on whether and under what circumstances it should revoke any existing authorization of equipment that poses an unacceptable risk to our national security, as listed on the Commission's *Covered List*.[6] 5G Americas believes it would be a dangerous precedent to issue a blanket rescission of an existing authorization for telecommunications equipment that otherwise complies with the Commission's other requirements. 5G Americas does not object to requiring existing authorized equipment providers to provide a local contact for service of process or inquiries from the FCC.[7] But a blanket rescission of existing authorizations, however worthy the security goal, would undermine trust in the Commission's processes.

Long-term, there could be an inhibitive effect as developers of innovative equipment choose to introduce their devices, base stations, switches and components in markets outside the United States. The Commission, in implementing the *Secure and Trusted Networks Act*, already will require every telecom provider to report whether they have covered equipment in their network. The Commission can follow up, as appropriate, with providers that positively report to identify and remediate any security threats to their networks caused by the presence of covered equipment. Such an approach would be less burdensome on the industry in the U.S., while preserving trust in the Commission's equipment authorization and the attractiveness of the U.S. market for the introduction of innovative equipment.

---

[5] *See Protecting Against National Security Threats* ¶¶ 3, 38, 40.

[6] *See List of Equipment and Services Covered By Section 2 of The Secure Networks Act*, FCC, https://www.fcc.gov/supplychain/coveredlist.

[7] *See Protecting Against National Security Threats* ¶54.

II. SECURE SOFTWARE AND PRACTICES REVIEW

In its *Notice of Inquiry*, the Commission seeks comment on actions the Commission should consider taking to create incentives to spur trustworthy innovation for more secure equipment.[8] Specifically, the Commission seeks comment on how it can leverage its equipment authorization program to encourage manufacturers requiring such authorization to consider cybersecurity standards and guidelines.[9] With respect, 5G Americas observes that communications equipment manufacturers have every incentive to adhere to the existing cybersecurity standards and guidelines that the Commission details in its NOI. There are strong market imperatives to ensure wireless equipment has state-of-the-art cybersecure software to be eligible for federal contracts, let alone to meet the private sector's demand for cybersecurity.

These incentives are increasing. Late last month, the White House hosted a meeting on improving cybersecurity in U.S. supply chains at which a number of leading technology companies made commitments that will have downstream effects in the ecosystem. For instance, a leading cybersecurity insurer committed to only offering insurance coverage to companies meeting a certain minimum standard of cyber best practices.[10] At the August White House meeting, the National Institute for Standards and Technology ("NIST") promised to develop a new framework focused on improving the technical supply chain security. Moreover, as the Commission notes, in May 2021, President Biden issued an *Executive Order on Improving the Nation's Cybersecurity* ("EO").[11] The EO directs that the Commerce Department, through NIST, initiate a pilot on

---

[8] *Protecting Against National Security Threats* ¶¶ 3, 98.

[9] *Id.* ¶ 98.

[10] *See* News Staff, *Google, Microsoft Pledge Billions After White House Meeting*, Gov't Tech. (August 27, 2021), https://www.govtech.com/workforce/google-microsoft-pledge-billions-after-white-house-meeting.

[11] Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 12, 2021).

Internet of Things ("IoT") consumer product labeling to educate the public on the security of IoT devices and consumer software, in coordination with the Chair of the Federal Trade Commission ("FTC").[12] Notably, the EO does not provide a role to the FCC in enhancing cybersecurity of IoT devices and software development. NIST is also still in the process of developing the IoT Cybersecurity Improvement Act applicable guidelines for IoT Federal Procurement (NISTIR 8259D, and related SP), to be followed by Office of Management and Budget ("OMB") action. Both efforts build on NIST's voluntary, consensus-driven efforts in this area, such as the development of NISTIR 8259 series. Relatedly, the broadband division of the Senate's infrastructure bill provides funding to eligible entities for cybersecurity resources and programs available through federal agencies, including the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA"), NIST and the FTC.[13] The FCC is not mentioned with respect to enhancing the cybersecurity of broadband networks or devices in this latest articulation of congressional intent on the Commission's proper role in securing the communications supply chain.

Several years ago, NIST convened stakeholders to develop a Cybersecurity Framework that addresses threats and supports business. The Framework integrates industry standards and best practices to help organizations manage their cybersecurity risks. The Framework not only helps organizations understand their cybersecurity risks (threats, vulnerabilities and impacts), but how to reduce these risks with customized measures. The Framework also helps them respond to and

[12] *Id.* 26,637–26,642.

[13] *See Infrastructure Investment and Jobs Act*, H.R.3684, 117th Cong. § 60102(b)(4)(B)(ii). The infrastructure bill also allocates $1 Billion by 2025 (§ 70612 (r)(1), 2289) specifically to fund grants to state and local governments adopting cybersecurity best practices and names NIST's cybersecurity framework as a guide for state and local entities to follow (§70612 (e)(2)(B)(v)(I), 2260).

recover from cybersecurity incidents, prompting them to analyze root causes and consider how they can make improvements.[14]

5G Americas supports voluntary industry progress toward a Zero Trust Architecture, and NIST's guidance on Zero Trust. 5G Americas has encouraged operators deploying 5G to take a Zero-Trust approach, which can be combined with the advanced techniques of cyber threat intelligence and Network Slicing that 5G offers to further enhance 5G's security.[15] NIST's actions and federal agencies' adoption of Zero Trust are more than sufficient, and the Commission's proposed efforts to further encourage equipment vendors to adhere to IoT cybersecurity standards would more likely be duplicative or distracting, rather than actually improving the cybersecurity of broadband equipment or its supply chain.

CISA has an existing and complex structure for interfacing with the private sector towards the goal of increasing the country's cybersecurity. As they describe their role:

> In accordance with Presidential Policy Directive 21 (PPD-21) and the 2013 National Infrastructure Protection Plan (NIPP), CISA's Stakeholder Engagement and Cyber Infrastructure Resilience Division (SECIR) serves as the Sector Risk Management Agency (SRMA) for the Information Technology (IT) and Communications critical infrastructure sectors. As detailed in the NIPP, SRMAs coordinate efforts across the critical infrastructure community to strengthen the security and resilience of their sectors, serve as the Federal interface for sector-specific activities, carry out incident management responsibilities

[14] *See* Nat'l Inst. for Stands. and Tech., Framework for Improving Critical Infrastructure Cybersecurity, at v-vi (2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[15] See 5G Americas, *Security Considerations for the 5G Era* (July 2020) at 46.

consistent with statutory authority, support and facilitate technical assistance to identify sector vulnerabilities, and support annual reporting requirements.

The Communications SRMA accomplishes these missions by serving as the focal point for coordination in the private-public partnership model, working with Sector Coordinating Councils (SCC); Government Coordinating Councils (GCC); the SLTT GCC; the Critical Infrastructure Cross-Sector Council; the Federal Senior Leadership Council; the Regional Consortium Coordinating Council; and information sharing organizations (e.g., Information Sharing and Analysis Centers). In addition to supporting the communications (and information technology) industry, the IT and Communications SRMA provides information across the critical infrastructure community to increase the security and resilience of the Nation's critical infrastructure.[16]

Moreover, CISA was recently strengthened, including by the creation of a Joint Cyber Defense Collaboration[17] and the Joint Cyber Planning Office, which brings together "major cloud providers, cyber companies, and other private sector partners under a new initiative aimed at combining efforts on planning, threat analysis, and defensive operations."[18] The 2021 Fiscal Year

[16] *Stakeholder Engagement and Cyber Infrastructure Resilience*, Cybersec. and Infrast. Sec. Agency, https://www.cisa.gov/stakeholder-engagement-and-cyber-infrastructure-resilience

[17] *See* Jule Pattison-Gordon, *Cyberspace Solarium Commission Reports on Recent Progress*, Gov't Tech., Aug. 12, 2021, https://www.govtech.com/security/cyberspace-solarium-commission-reports-on-recent-progress.

[18] Justin Doubleday, *CISA Looks to ties together public-private partnerships through new cyber planning office*, Fed. News Network, Aug. 5, 2021, https://federalnewsnetwork.com/cybersecurity/2021/08/cisa-looks-to-tie-together-public-private-partnerships-through-new-cyber-planning-office/.

National Defense Authorization Act provided that the Joint Cyber Planning Office will continue for the foreseeable future.[19]

In addition to CISA, the Department of Homeland Security ("DHS") has a number of other offices and programs designed to encourage the private sector to employ best practices for cybersecurity. DHS' Critical Infrastructure Cyber Community Voluntary Program (C^3 Voluntary Program) is a "focal point for cybersecurity outreach and information" for the sixteen sectors of critical infrastructure in the United States, including information technology and communications.[20] The C^3 Voluntary Program also serves small and midsize businesses. The C^3 Voluntary Program promotes use of NIST's Cybersecurity Framework, as well as a range of DHS cybersecurity tools, best practices, and services.

DHS also offers Cybersecurity Advisors (CSAs) to help prepare and protect private sector entities from cybersecurity threats.[21] CSAs "promote cybersecurity preparedness, risk mitigation, and incident response capabilities, working to engage stakeholders through partnership and direct assistance activities" including through cyber resilience reviews, working group support and partnership development. DHS also offers cybersecurity training exercises and workforce development, which can act as an incentive for software vendors to deploy best practices.

The May 2021 EO also empowered the National Telecommunications and Information Administration ("NTIA"), in conjunction with NIST, to continue work on its Software Bill of

---

[19] *See* Jule Pattison-Gordon, *Cyberspace Solarium Commission Reports on Recent Progress*, Gov't Tech., Aug. 12, 2021.

[20] *See Stakeholder Engagement and Cyber Infrastructure Resilience,* Cybersec. and Infrast. Sec. Agency, https://www.cisa.gov/stakeholder-engagement-and-cyber-infrastructure-resilience.

[21] *See id.*

Materials ("SBOM") process.[22] In July, pursuant to the EO, NTIA published a report on minimum elements for SBOM. The report focuses on modernizing U.S. cybersecurity defense infrastructure by "protecting Federal networks, improving information sharing between the U.S. Government and the private sector on cyber issues, and strengthening the United States' ability to respond to incidents when they occur."[23] The minimum elements as defined in NTIA's July report are the essential pieces of information that support basic SBOM functionality and are intended to "serve as the foundation for an evolving approach to software transparency."[24] The Report builds on work NTIA has been doing since at least 2019 to improve software transparency and provide guidance to interested parties based on collaboration between public and private entities through its Multi Stakeholders Group.[25]

As noted above, the May 12 EO tasked NIST and the FTC to coordinate on the release of criteria for a Consumer IoT Cybersecurity labeling pilot program, building on NISTIR 8259 foundational work, and this work is already underway.[26] NIST is also in the process of releasing

[22] Exec. Order No. 14028, 86 Fed. Reg. 26633, § 4(e)(7) at 26638. An SBOM is a formal record of the supply chain relationships of various components used in building software and other details.

[23] Natl' Telecomm. and Info. Admin., The Minimum Elements for a Software Bill of Materials (SBOM) (2021), https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf.

[24] *Id*.

[25] *See NTIA Software Component Transparency,* Natl' Telecomm. and Info. Admin., https://ntia.gov/SoftwareTransparency.

[26] *See IoT Device Criteria*, Nat'l Inst. of Standards and Tech., https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/iot-device-criteria (last visited Sept. 20, 2021).

relevant guidelines for the implementation of the *IoT Cybersecurity Improvement Act*, to be followed by additional OMB action.[27]

Likewise, the Department of Energy ("DOE") has an existing office focused on cybersecurity, the Office of Cybersecurity, Energy Security and Emergency Response ("CESER"). Many IoT devices that run on wireless networks are designed to work with both enterprise electrical systems and residential appliances. CESER encourages engineers and researchers to think about cyber defenses during initial development and design work so that security is ingrained from the beginning.[28] The office also helps test certain suppliers' offerings down to the chip and firmware level to catch any vulnerabilities before the products are adopted. Additional federal activities in this space would add costs without cybersecurity benefits.[29]

In addition to these federal civilian agencies, the Department of Defense is an important buyer in the software marketplace, including for IoT and other devices and systems that run on broadband networks. DoD developed the Cybersecurity Maturity Model Certification ("CMMC"), which is a unified security standard and a certification process that significantly enhances

---

[27] Nat'l Inst. of Standards and Tech., NISTIR 8379, Summary Report for the Virtual Workshop Addressing Public Comment on NIST Cybersecurity for IoT Guidance (2021), https://csrc.nist.gov/publications/detail/nistir/8379/final.

[28] *See generally Cybersecurity*, Off. of Cybersec., Energy Sec., and Emergency Response, https://www.energy.gov/ceser/cybersecurity.

[29] If anything, federal officials responsible for cybersecurity incident reporting would prefer a more centralized approach, rather than having separate reporting regimes for different sectors. *See* Jule Pattison-Gordon, *Congress Analyzes Security of Vulnerable U.S. Electric Grid*, Gov't Tech., July 29, 2021, https://www.govtech.com/security/congress-analyzes-security-of-vulnerable-u-s-electric-grid, noting remarks of CISA Executive Assistant Director for Cybersecurity, Eric Goldstein ("sector-by-sector approach to policy-setting can result in inconsistencies and blind spots that inhibit federal agencies' efforts to track threats and warn all potentially impacted parties." A sector-based approach can lead to various sectors defining cyber incidents differently and establishing different reporting deadlines, making it difficult for CISA to get clear, comparable insights and less able to assist victims, warn other potential targets and understand new threats).

cybersecurity across industries that supply to DoD and its service branches. CMMC is a critical component of heightened security that is expected to have a profound impact on DoD contracting, requiring all prime and sub-contractors doing business with DoD to achieve a CMMC certification level as a prerequisite to new contract awards.[30]

Adding an additional layer of federal agency requirements through an FCC certification or other process does not appear to be necessary and 5G Americas advises against that course.

5G Americas understands that IoT devices connected to various types of networks have unfortunately been the victim of hacks, similar to many other layers of the ICT supply chain and connected devices, and the mobile communications industry needs to be vigilant with mechanisms to defend against fraudulent activity. Typically, attacks on IoT or on IT systems are the product of scams, phishing, email Trojan Horses, insecure servers, etc. Nonetheless, 5G, as well as the connected-device IoT ecosystem, has benefitted from active developments in the standards-setting process, as well as from security innovations. By way of example, 3GPP Release 17 has a number of real-world improvements for enhanced security folded into its requirements, such as with network slicing, and having each Extensible Authentication Protocol hop mutually authenticated, while providing confidentiality and integrity checks.[31] Given the activities of a number of federal agencies on cybersecurity, and the focus by industry standards bodies on 5G security, an additional federal regulator in this space would add regulatory burdens and create

[30] *See generally* Off. of the Under Sec'y of Def. for Acquisition and Sustainment, *Cybersecurity Maturity Model Certification*, https://www.acq.osd.mil/cmmc/.

[31] See 5G Americas, *Security Considerations for the 5G Era* (July 2020) at 25, available at https://www.5gamericas.org/security-considerations-for-the-5g-era/.

uncertainty, without commensurate improvements in the trusted innovation the Commission seeks.[32]

CONCLUSION

5G Americas appreciates the Commission's efforts to date to make U.S. networks more secure. Cyber security across all U.S. networks is such a broad and complex area, and developments in cyber security so dynamic, that 5G Americas cautions the Commission against using its equipment authorization program – which can be a quite lengthy process - to regulate cyber security. Rather, 5G Americas points the Commission to collaborating with and leveraging the extensive cyber security guidance issued by other federal government partners, including NIST and CISA. In addition, 5G Americas suggests the Commission look to existing forums under its authority, such as by tasking the Commission's federal advisory council, the Communications Security, Reliability and Interoperability Council ("CSRIC VIII") to provide the Commission with recommendations on how to improve cyber security within U.S. telecom networks including through FCC-authorized equipment. Under Commission leadership, CSRIC has provided it with a number of valuable recommendations over the last several years. The Commission should use comments in this proceeding to shape additional areas for which the recently revitalized CSRIC VIII should develop Recommendations for Commission action consistent with its authority and its role relative to the numerous other federal agencies tasked with cyber security responsibility in legislation or Executive Orders.

[32] Executive Order 14028 itself appears to disapprove of sector-specific cybersecurity measures, noting that agency-specific policies and regulations have led to some weaknesses in the Nation's overall threat preparedness, instead calling for standardizing common cybersecurity requirements across agencies to streamline and improve compliance. See Exec. Order No. 14028, 86 Fed. Reg. 26633, §2(h) at 26635.