May 27, 2021

FCC FACT SHEET[*]

Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program; Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program

Notice of Proposed Rulemaking and Notice of Inquiry, ET Docket No. 21-232, EA Docket No. 21-233

Background: Over the last few years, the Commission, Congress, and the Executive Branch all have taken action to protect the supply chain for communications equipment and services within the United States. This Notice of Proposed Rulemaking and Notice of Inquiry furthers the Commission's goal of protecting our communications networks and supply chains from equipment and services that pose an unacceptable risk to national security by amending our rules related to equipment authorization and competitive bidding.

What the *Notice of Proposed Rulemaking* Would Do:

- Seek comment on a proposal to prohibit all future authorizations for equipment on the Covered List promulgated by the Commission pursuant to the Secure and Trusted Communications Networks Act of 2019.
    - This includes equipment subject to the FCC's certification and Supplier's Declaration of Conformity processes associated with equipment authorization.
- Seek comment on whether to revise the FCC's rules on equipment currently exempted from the equipment authorization requirements to no longer permit this exemption for equipment on the Covered List.
- Seek comment on whether to revoke authorizations that previously have been granted for equipment on the Covered List.
- Seek comment on a proposal to require applicants who wish to participate in Commission auctions to certify that their bids do not and will not rely on financial support from any entity that the Commission has designated under Section 54.9 of the FCC's rules as a national security threat to the integrity of communications networks or the communications supply chain.

What the *Notice of Inquiry* Would Do:

- Seek comment on how the Commission can leverage its equipment authorization program to encourage manufacturers who are building devices that will connect to U.S. networks to consider cybersecurity standards and guidelines.

[*] This document is being released as part of a "permit-but-disclose" proceeding. Any presentations or views on the subject expressed to the Commission or its staff, including by email, must be filed in ET Docket No. 21-232 and OEA Docket No. 21-233, which may be accessed via the Electronic Comment Filing System (https://www.fcc.gov/ecfs/). Before filing, participants should familiarize themselves with the Commission's ex parte rules, including the general prohibition on presentations (written and oral) on matters listed on the Sunshine Agenda, which is typically released a week prior to the Commission's meeting. *See* 47 CFR § 1.1200 et seq.

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
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program	)	EA Docket No. 21-233
	)	

NOTICE OF PROPOSED RULEMAKING AND NOTICE OF INQUIRY*

Adopted: "Insert Adopted Date" **Released: "Insert Release Date"**

Comment Date: 30 days after Federal Register Publication
Reply Comment Date: 60 days after Federal Register Publication

By the Commission:

TABLE OF CONTENTS

* This document has been circulated for tentative consideration by the Commission at its June 2021 open meeting. The issues referenced in this document and the Commission's ultimate resolutions of those issues remain under consideration and subject to change. This document does not constitute any official action by the Commission. However, the Acting Chairwoman has determined that, in the interest of promoting the public's ability to understand the nature and scope of 4 issues under consideration, the public interest would be served by making this document publicly available. The Commission's *ex parte* rules apply and presentations are subject to "permit-but-disclose" *ex parte* rules. *See, e.g.*, 47 CFR §§ 1.1206, 1.1200(a). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules, including the general prohibition on presentations (written and oral) on matters listed on the Sunshine Agenda, which is typically released a week prior to the Commission's meeting. *See* 47 CFR §§ 1.1200(a), 1.1203.

I. INTRODUCTION

1. The Commission plays an important role in protecting the security of America's communications networks. Recently, the Commission, Congress, and the Executive Branch have taken action to protect the supply chain of equipment and services within the United States. The Commission, in particular, has taken a number of targeted steps to ensure that public funds are not used in a way that undermines or poses a threat to our national security.

2. Today, we build on those efforts. In this proceeding, consistent with concurrent Congressional and Executive Branch actions, we explore steps we can take to further the Commission's goal of protecting our communications networks from communications equipment and services that pose a national security risk or a threat to the safety of U.S. persons beyond the Commission's universal service programs. Specifically, we propose that the Commission's rules related to equipment authorization and our competitive bidding procedures also can play an important role in securing our nation's critical communications networks, and we seek comment on how we should review and revise these processes for this purpose. Our action is guided by the belief that the Commission must do all it can within its legal authority to address national security threats.

3. In particular, in the Notice of Proposed Rulemaking (Notice), we propose prohibiting the authorization of any equipment on the list of equipment and services (Covered List) that the Commission maintains pursuant to the Secure and Trusted Communications Networks Act of 2019.[1] Such equipment has been found to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons. We also seek comment on whether and under what circumstances we should revoke any existing authorizations of such "covered" communications equipment. Finally, we invite comment on whether we should require additional certifications relating to national security from applicants who wish to participate in Commission auctions. In the Notice of Inquiry, we seek comment on other actions the Commission should consider taking to create incentives in its equipment authorization processes for improved trust through the adoption of cybersecurity best practices in consumer devices.

4. The Commission has reviewed and revised its equipment authorization and competitive bidding processes through the years to meet the challenges of an evolving ecosystem. While we are

[1] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609) (Secure Networks Act). The Commission's Public Safety and Homeland Security Bureau (PSHSB) maintains the list at https://www.fcc.gov/supplychain/coveredlist.

taking action in this Notice to leverage these processes to help keep untrusted vendors and equipment out of U.S. networks, the Commission also is taking action to review and revise these processes to spur trustworthy innovation that can advance the nation's global competitiveness and promote responsible global development and deployment. We are doing so by streamlining equipment authorization so that the American public can benefit more quickly from new and more advanced communications systems that rely on this equipment, while still ensuring that the important goals of the equipment authorization system and security are not undermined.[2] Together, these actions advance the Commission's comprehensive strategy to help build a more secure, resilient, and next-generation communications supply chain.

II. BACKGROUND

5. In this Notice of Proposed Rulemaking and Notice of Inquiry, we build upon the Commission's efforts to reduce the presence of untrusted equipment in United States communications networks. In this Background section, we begin by discussing the Commission's actions to date, which recently have culminated in new rule provisions to promote more secure networks along with the publication, in March of this year, of a list of "covered" equipment and services that have been deemed to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons.[3] We then discuss the Commission's part 2 equipment authorization rules and processes through which the Commission authorizes equipment for operation in the United States. The Commission's current rules do not yet include provisions that address the authorization of such "covered" equipment. Finally, we review how application certifications required by the Commission's part 1 competitive bidding rules serve to protect against the risk of future harms to the public interest and how such certifications might be used to mitigate the risks to U.S. communications networks and services.

A. Recent Commission Actions, as well as Congressional and Executive Branch Actions, to Protect the Security of our Nation's Communications System

6. At an increasingly rapid pace in recent years, the United States government has moved to protect the security of the communications networks across our nation. Congress and the Executive Branch have prioritized the importance of identifying and eliminating potential security vulnerabilities in communications networks and their supply chains.[4] The Commission, which was created by Congress in

[2] *Allowing Earlier Equipment Marketing and Importation Opportunities*, ET Docket No. 20-382, Report and Order, FCC 21-xxx (June 17, 2021) (adopting targeted enhancements that will modernize the Commission's marketing and importation rules to allow equipment manufacturers to better gauge consumer interest and prepare for new product launches in order to further the communication's sector's ability to drive innovation and promote economic growth).

[3] "Public Safety and Homeland Security Bureau Announces Publication of the List of Equipment and Services Covered by Section 2 of the Secure Networks Act," WC Docket No. 18-89, Public Notice, DA 21-309 (PSHSB, Mar. 12, 2021) (*Covered List Public Notice*); *see* 47 CFR § 1.50002.

[4] In 2012, the House Permanent Select Committee on Intelligence released a bipartisan report assessing the counterintelligence and security threat posed by Chinese telecommunications companies operating in or providing equipment to customers in the United States. Permanent Select Committee on Intelligence, U.S. House of Representatives, Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE at iv (Oct. 8, 2012), https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huaweizte%20investigative%20report%20(final).pdf. In November 2018, the Department of Homeland Security convened the Information and Communications Technology Supply Chain Risk Management Task Force, a public-private partnership formed to examine and develop consensus recommendations to identify and manage risk to the global information and communications supply chain. Press Release, Department of Homeland Security, DHS Announces ICT Supply Chain Risk Management Task Force Members (Nov. 15, 2018), https://www.dhs.gov/news/2018/11/15/dhs-announces-ict-supply-chain-riskmanagement-task-force-members. In 2020, the Department of Defense explained its strategic objective for supply chain security is to "[r]educe threats to key U.S. supply chains to prevent foreign attempts to compromise the integrity, trustworthiness, and authenticity of products and services purchased and integrated into the operations of the U.S. Government, the Defense Industrial Base, and the private sector." The National Counterintelligence and Security Center, Supply

(continued….)

part "for the purpose of the national defense [and] for the purpose of promoting safety of life and property through the use of wire and radio communication . . . ,"[5] in turn has helped to identify and address these vulnerabilities by using its resources in taking various actions to protect the integrity of communications networks and the communications supply chain.

7. *Congressional and Executive Branch Action Prior to the Secure and Trusted Communications Networks Act of 2019*. Over the years, both Congress and the Executive Branch have taken numerous actions to identify and address threats to our nation's communications systems posed by certain communications equipment. In 2013, the White House issued Executive Order 13636, which directed the National Institute of Standards and Technology (NIST) to begin working with stakeholders to develop a voluntary cybersecurity framework designed to reduce risks to critical infrastructure.[6] In May 2017, the White House released Executive Order 13800, which directed the Secretary of Homeland Security, in coordination with the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the Federal Bureau of Investigation, and all other appropriate agency heads, to identify authorities and capabilities that agencies could employ to support the cybersecurity efforts of critical infrastructure entities, and to determine how best to support cybersecurity risk management efforts.[7]

8. In December 2017, Congress enacted the National Defense Authorization Act for Fiscal Year 2018 (2018 NDAA), which included provisions that addressed continuing concerns over the purchase and use of certain communications equipment, specifically barring the Department of Defense from using telecommunications equipment or services produced or provided by Huawei Technologies Company or ZTE Corporation for certain critical programs, including ballistic missile defense and nuclear command, control, and communications.[8] In August 2018, Congress enacted the National Defense Authorization Act for Fiscal Year 2019 (2019 NDAA),[9] which, pursuant to Section 889(b)(1) prohibits the head of an Executive Branch agency from using federal funds to procure or obtain equipment, services, or systems that use "covered telecommunications equipment or services" as a substantial or essential component of any system, or as critical technology as part of any system.[10] Section 889(f)(3) of the 2019 NDAA subsequently and generally defines "covered telecommunications equipment or services" as (1) telecommunications equipment produced by Huawei or ZTE or any subsidiary or affiliate of such entities; (2) for certain safety and security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation (Hytera), Hangzhou Hikvision Digital Technology Company (Hikvision), or Dahua Technology Company (Dahua) or any subsidiary or affiliate of such entities; (3) telecommunications or video surveillance equipment services provided by such entities or using such equipment; or (4) telecommunications or video surveillance equipment or services produced by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country, where

Chain Risk Management: Reducing Threats to Key U.S. Supply Chains (Sept. 25, 2020), https://www.dni.gov/files/NCSC/documents/supplychain/20200925-NCSC-Supply-Chain-Risk-Management-tri-fold.pdf.

[5] 47 U.S.C. § 151.

[6] Exec. Order No. 13636, 78 Fed. Reg. 11737 (Feb. 19, 2013).

[7] Exec. Order No. 13800 § 2(b), 82 Fed. Reg. 22391, 22393, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 11, 2017).

[8] *See* Pub. L. 115-91, 131 Stat. 1283, 1762, § 1656.

[9] *See* Pub. L. 115-232, 132 Stat. 1636.

[10] *Id*. at 1917, § 889(a)-(b)(1).

"covered foreign country" is defined as the People's Republic of China.[11]

9. In December 2018, Congress enacted the SECURE Technology Act to create the Federal Acquisition Security Council, which includes seven Executive Branch agencies.[12] The Council is charged with developing a government-wide strategy to address communications supply chain risks and may recommend that other agencies remove insecure communications services or equipment.[13] In May 2019, the White House issued Executive Order 13873, declaring a national emergency with respect to the security, integrity, and reliability of information and communications technology and services, and granting the Secretary of Commerce the authority to prohibit transactions of information and communications technology or services when, among other things, the transaction would pose undue risks to U.S. critical infrastructure or national security.[14] In November 2019, the Department of Commerce began a rulemaking to implement Executive Order 13873.[15]

10. *Commission Action Prior to Enactment of the Secure and Trusted Communications Networks Act of 2019*. In 2018, the Commission took new steps to protect communications networks and supply chains from communications equipment and services that could pose a national security risk. In April 2018, the Commission adopted a new proceedings, WC Docket No. 18-89, proposing to prohibit the use of Universal Service Fund (USF) support to purchase or obtain equipment or services from any communications equipment or service provider identified as posing a national security risk to communications networks or the communications supply chain.[16] In November 2019, the Commission adopted the *USF Supply Chain Report and Order, Further Notice, and Order*, in which it adopted a rule prohibiting the use of "universal service support . . . to purchase or obtain any equipment or services produced or provided by a covered company posing a national security threat to the integrity of communications networks or the communications supply chain."[17] The Commission also initially designated two Chinese companies, Huawei and ZTE, and their subsidiaries, parents, or affiliates, as companies that pose a national security threat to the integrity of communications networks and the communications supply chain, and we established a process for future designations of other companies

[11] *Id*. at 1918, § 889(f)(2)-(3).

[12] *See* Pub. L. 115-390, 132 Stat. 5173.

[13] *See id.*

[14] *See* Exec. Order No. 13873, 84 Fed. Reg. 11578, Executive Order on Securing the Information and Communications Technology and Services Supply Chain (May 15, 2019), https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/ (Executive Order 13873). On May 14, 2020, the President issued an order extending the emergency declaration for another year. *See* Continuation of the National Emergency with Respect to Securing the Information and Communications Technology and Services Supply Chain, 85 Fed. Reg. 29321 (May 14, 2020).

[15] U.S. Department of Commerce, Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65316 (Nov. 27, 2019).

[16] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Notice of Proposed Rulemaking, 33 FCC Rcd 4058, 4058, para. 2 (2018) (*USF Supply Chain Notice*).

[17] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423, 11433, para. 26 (2019) (*USF Supply Chain Order and Further Notice*), *appeal pending in Huawei Technologies USA v. FCC*, No. 19-60896 (5th Cir.). The Commission adopted this rule based on its conclusion that it is critical to the provision of "quality service," 47 U.S.C. § 254(b)(1), that USF support be spent on secure networks and not on equipment and services from companies that threaten national security. Pursuant to this rule, which is codified at 47 CFR § 54.9, USF support may not be used to purchase, maintain, improve, modify, operate, manage, or otherwise support any equipment or services produced or provided by a covered company.

posing such a risk.[18] Consistent with that process,[19] the Commission's Public Safety and Homeland Security Bureau issued final designations of Huawei and ZTE on June 30, 2020,[20] which immediately precluded use of USF support to purchase, maintain, improve, modify, operate, manage, or otherwise support any equipment or services produced or provided by Huawei or ZTE or their subsidiaries, parents, or affiliates.[21]

11. The Commission also has taken action, by authority of section 214 of the Communications Act, to protect our communications networks.[22] In 2019, the Commission declined to grant China Mobile's application for a section 214 authorization to provide international telecommunications services between the U.S. and foreign destinations because it concluded that the company was "vulnerable to exploitation, influence, and control by the Chinese government."[23] Relying on the expertise of appropriate Executive Branch agencies, the Commission concluded that there existed "a significant risk that the Chinese government would use the grant of such authority to [the carrier] to conduct activities that would seriously jeopardize the national security and law enforcement interests of the United States."[24] In 2020 and 2021, the Commission has also been considering whether other carriers

[18] *See USF Supply Chain Order*, 34 FCC Rcd at 11438-48, paras. 43-63.

[19] *See USF Supply Chain Order*, 34 FCC Rcd at 11438, para. 40; *id.* at 11449, para. 64; *id.* at 11486, para. 185 (directing the Public Safety and Homeland Security Bureau to determine whether to finalize the initial designations within 120 days of the *Order*'s publication in the Federal Register, and holding that the Bureau may extend the 120-day deadline for good cause); *Public Safety and Homeland Security Bureau Extends Timeframe For Determining Whether to Finalize Designations of Huawei and ZTE Pursuant to 47 CFR § 54.9*, PS Docket Nos. 19-351 and 19-352, Public Notice, 35 FCC Rcd 4515 (PSHSB 2020) (finding good cause to extend the timeframe for determining whether to finalize the initial designations of Huawei and ZTE to June 30, 2020).

[20] *See generally Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation*, PS Docket No. 19-351, Order, 35 FCC Rcd 6604 (PSHSB 2020) (*Huawei Designation Order*); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – ZTE Designation*, PS Docket No. 19-352, Order, 35 FCC Rcd 6633 (PSHSB 2020) (*ZTE Designation Order*).

[21] In the *USF Supply Chain Further Notice* portion, the Commission sought comment on a proposal to "require, as a condition on the receipt of any USF support that Eligible Telecommunications Carriers [ETCs] not use or agree not to use within a designated period of time, communications equipment or services from covered companies." *USF Supply Chain Order*, 34 FCC Rcd at 11470–71, para. 122. It also proposed to establish a program to reimburse costs incurred by ETCs required to remove and replace covered equipment and services. *Id.* To better inform the Commission's consideration of a reimbursement program and the presence of Huawei and ZTE equipment in U.S. networks, the *Information Collection Order* portion of its decision, which required ETCs to report whether they use or own Huawei or ZTE equipment or services in their networks, or the networks of their affiliates and subsidiaries, and to report the cost of removing and replacing such equipment and services. *Id.* at 11481–82, paras. 162–63. The Commission released the results of that information collection in September 2020. *See Wireline Competition Bureau and Office of Economics and Analytics Release Results from Supply Chain Security Information Collection*, WC Docket No. 18-89, Public Notice, 35 FCC Rcd 9471 (WCB 2020) (Information Collection Results PN).

[22] 47 U.S.C. § 214(a) ("No carrier shall undertake the construction of a new line or an extension of any line, or shall acquire or operate any line, or extension thereof, or shall engage in transmission over or by means of such additional or extended line, unless and until there shall first have been obtained from the Commission a certificate that the present or future public convenience and necessity require or will require the construction, or operation, or construction and operation, of such additional or extended line . . . ."); *see also* China Mobile International (USA) Inc.; Application for Global Facilities-Based and Global Resale International Telecommunications Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended, File No. ITC-214-20110901-00289; *China Mobile International (USA) Inc.*, Memorandum Opinion and Order, 34 FCC Rcd 3361, 3365-66, para. 8 (2019) (*China Mobile USA Order*).

[23] *China Mobile USA Order*, 34 FCC Rcd at 3365-66, para. 8.

[24] *Id.*

affiliated with the Chinese government that hold international section 214 authority should continue to be authorized to provide telecommunications service in the United States.[25]

12. *Secure and Trusted Communications Networks Act of 2019*. On March 12, 2020, the President signed into law the Secure and Trusted Communications Networks Act of 2019 (the Secure Networks Act).[26] The Secure Networks Act intersects with several key provisions of the Commission's USF Supply Chain proceeding (WC Docket No. 18-89). A core provision of the Secure Networks Act – Section 2 – mandates that the Commission publish, and periodically update, a list of "covered communications equipment and services" (Covered List) that have been determined to pose national security risks.[27]

13. Other provisions of the Secure Networks Act prohibit the use of USF support to purchase "covered" communications equipment or services (section 3) and direct the Commission to establish a reimbursement program (section 4) substantially similar to the one proposed in the *USF Supply Chain Further Notice*.[28] Under the reimbursement program, the Commission will make reimbursement to providers of advanced communications services to remove and replace "covered" equipment and services, and develop an application process for providers to obtain the reimbursement.[29] Among other things, applicants for reimbursement are required to certify that, if their applications are approved, "in developing

[25] *See Pacific Networks Corp. and ComNet (USA) LLC*, GN Docket 20-111, Order Instituting Proceedings on Revocation and Termination, FCC 21-28 (Mar. 19, 2021); *China Unicom (Americas) Operations Limited*, GN Docket 20-110, Order Instituting Proceeding on Revocation, FCC 21-37 (Mar. 19, 2021); *China Telecom (Americas) Corporation*, GN Docket No. 20-109, Order Instituting Proceedings on Revocation and Termination and Memorandum Opinion and Order, 35 FCC Rcd 15006 (2020). *See also China Telecom (Americas) Corp. v. FCC*, No. 20-2365, Order (4th Cir. May 10, 2021) (appeals court unanimously dismissing China Telecom's challenge to the Commission's decision to institute proceedings to decide whether to revoke and terminate international section 214 authority on national security grounds, because the Commission's decision was not a final agency action).

[26] Secure Networks Act, *supra* note 1.

[27] Secure Networks Act § 2. Specifically, to be "covered," the Secure Networks Act provides that such equipment must meet two criteria. First, the communications equipment or service must, based exclusively on determinations made by Congress, certain government agencies, or interagency bodies, "pose[] an unacceptable risk to the national security of the United States or the security and safety of United States persons[.]" Secure Networks Act § 2(b)(1). Second, the equipment or services must be "capable of—(A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles; (B) causing the network of a provider of advanced communications service to be disrupted remotely; or (C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons." *See id.* § 2(a).

[28] Section 3 of the Secure Networks Act prohibits the use of "a Federal subsidy that is made available through a program administered by the Commission and that provides funds to be used for the capital expenditures necessary for the provision of advanced communications service" to purchase, rent, or otherwise obtain any covered communications equipment or services published on the list established pursuant to section 2. *See* Secure Networks Act § 3(a)(1)(A)-(B). Consistent with the Commission's proposals in the *USF Supply Chain Further Notice*, section 4 of the Secure Networks Act establishes the Secure and Trusted Communications Networks Reimbursement Program (Reimbursement Program) to facilitate the removal, replacement, and disposal of covered communications equipment and services, complete with reporting and certification requirements. *See id.* § 4(a). Section 5 requires all providers of "advanced communications services" to submit annual reports to the Commission "regarding whether such provider has purchased, rented, leased, or otherwise obtained any covered communications equipment or service . . . ." *See id.* § 5(a). This reporting requirement is limited to equipment or services purchased after August 14, 2018. *See id.* Section 7 tasks the Commission with enforcing the Secure Networks Act and adds penalties beyond those in the Communications Act and our rules for violations of section 4. *See id.* § 7. Section 9 sets forth definitions of certain terms in the Secure Networks Act, including "advanced communications service" and "communications equipment or service." *See id.* § 9.

[29] Secure Networks Act § 4(a).

and tailoring the risk management … [they] will consult and consider the standards, guidelines, and best practices set forth in the cybersecurity framework developed by the National Institute of Standards and Technology."[30]

14. *Recent Commission Action.* In July 2020, the Commission released its *USF Supply Chain Declaratory Ruling and Second Further Notice*, which found that the Commission's prohibition, codified at 47 CFR § 54.9, "is consistent with and substantially implements subsection 3(a) of the Secure Networks Act, which prohibits the use of federal funds on certain communications equipment and services."[31] In the *USF Supply Chain Second Further Notice* portion, the Commission sought comment on how other sections of the Secure Networks Act interact with the Commission's ongoing efforts to secure the communications supply chain.[32]

15. In December 2020, the Commission adopted the *USF Supply Chain Second Report and Order* to take further steps toward securing our communications networks and implementing provisions of the Secure Networks Act that apply to Commission action directed toward securing our nation's communications networks.[33] A core component of that decision concerns the creation and publication of the Covered List. The Commission explained that, consistent with its *USF Supply Chain Second Further Notice* and pursuant to section 2 of the Secure Networks Act, it was required to place on the Covered List "any communications equipment or service that poses an unacceptable risk to the national security of the United States or the security and safety of United States persons based solely on one or more of the following determinations," and then lists four sources for such determinations. These include: (1) "[a] specific determination made by any executive branch interagency body with appropriate national security expertise, including the Federal Acquisition Security Council;" (2) "[a] specific determination made by the Department of Commerce pursuant to Executive Order No. 13873 . . . relating to securing the information and communications technology and services supply chain;" (3) "[t]he communications equipment or service being covered telecommunications equipment or services, as defined in section 889(f)(3)" of the 2019 NDAA; or (4) "[a] specific determination made by an appropriate national security agency."[34] The Commission concluded that it had no discretion to disregard determinations from these enumerated sources, and that the Commission can accept determinations only from these four categories

[30] Secure Networks Act § 4(d)(4). Pursuant to Executive Order No. 13636, issued in February 2013), the National Institute of Standards and Technology (NIST) began working with stakeholders to develop a voluntary cybersecurity framework designed to reduce risks to critical infrastructure. Exec. Order No. 13636, 78 Fed. Reg. 11737 (Feb. 19, 2013); *see* Nat'l Inst. of Standards & Tech., *Cybersecurity Framework: New to Framework* (last updated Sept. 23, 2020), https://www.nist.gov/cyberframework/new-framework. This framework is "voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk." Nat'l Inst. of Standards & Tech., *Cybersecurity Framework: New to Framework*. NIST also has developed a Cybersecurity for the Internet of Things (IoT) program, which "supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed." Nat'l Inst. of Standards & Tech., *NIST Cybersecurity for IoT Program* (last updated Mar. 19, 2021), https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program.

[31] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Declaratory Ruling and Second Further Notice of Proposed Rulemaking, 35 FCC Rcd 7821, 7826-27, para. 20 (2020) (*2020 USF Supply Chain Declaratory Ruling and Second Further Notice*).

[32] *See id.* at 7828-39, paras. 23-60.

[33] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Second Report and Order, 35 FCC Rcd 14284 (2020) (*USF Supply Chain Second Report and Order*).

[34] *USF Supply Chain Second Report and Order*, 35 FCC Rcd at 14311-12, para. 58 (quoting the Secure Networks Act § 2(c)). The Act defines "appropriate national security agency" to include the Department of Homeland Security, the Department of Defense, the Office of the Director of National Intelligence, the National Security Agency, and the Federal Bureau of Investigation. *Id.* § 9(2).

of sources.[35] The Commission also noted that the "covered" equipment on the Covered List could identify specific pieces of equipment or include a class or category of equipment,[36] and that the Commission was not required to conduct a technical analysis of the equipment prior to including it on the Covered List.[37] The Commission provided that the Public Safety and Homeland Security Bureau, pursuant to delegated authority, would issue the Covered List and to provide updates or modifications to that list as appropriate,[38] and that the Covered List would be published without providing notice or opportunity to comment.[39]

16. In the *USF Supply Chain Second Report and Order*, the Commission adopted a new rule section, section 1.50000 *et seq*., to implement the Secure Networks Act. Section 1.50002 sets forth what communications equipment or service the Public Safety and Homeland Security Bureau must include on the Covered List.[40] That rule provides:

> § 1.50002(b). *Inclusion on the Covered List*. The Public Safety and Homeland Security Bureau shall place on the Covered List any communications equipment or service that:

---

[35] *USF Supply Chain Second Report and Order*, 35 FCC Rcd at 14312, para. 60 (citing the Secure Networks Act § 2(c) ("In taking action under subsection (b)(1), the Commission shall place on the list any communications equipment or service that poses an unacceptable risk to the national security of the United States or the security and safety of United States persons based solely on one or more of the following determinations . . . .")). *See also USF Chain Second Report and Order*, 35 FCC Rcd at 14312-16, paras. 61-70.

[36] The Commission also discussed how particular determinations would be incorporated onto the Covered List. If a determination indicates that a *specific* piece of equipment or service poses an unacceptable risk to the national security of the United States and the security and safety of United States persons, the Commission will automatically include this determination on the Covered List. The Commission concluded that if an enumerated source has already performed the analysis on whether the equipment or service poses an unacceptable risk to the national security of the United States or the security and safety of United States persons as part of its determination, the only action the Commission needs take is to incorporate this determination onto the Covered List. The Commission found that its actions in this scenario are non-discretionary and ministerial; that is, if the determination is specified to a particular piece of communications equipment or service, the Commission has no discretion to exclude that determination from the Covered List. *USF Supply Chain Second Report and Order*, 35 FCC Rcd at 14320-21, paras. 80-81. The Commission noted that if interested parties seek to reverse or modify the scope of one of the determinations, the party should petition the source of the determination. *USF Supply Chain Second Report and Order*, 35 FCC Rcd at 14324, para. 89. Meanwhile, with regard to *broader* determination, such as a class or category of communication equipment or service (*e.g*., "telecommunications equipment produced or provided by Huawei Technologies Company" or any subsidiary or affiliate), or telecommunications equipment that "is capable of (A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles, (B) causing the networks of a provider of advanced communications service to be disrupted remotely, or (C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons" – that broader category will be included on the Covered List. *USF Supply Chain Second Report and Order*, 35 FCC Rcd at 14321, paras. 82-83 (citing the Secure Networks Act §§ 2(b)(1); 2(b)(2)(A)-(C)). The Commission noted that, by adopting this approach and continuing to be deferential to the enumerated sources making the determination, the Commission will continue to work closely with Executive Branch entities with expertise and responsibilities concerning telecommunications security, including supply chain security. *USF Supply Chain Second Report and Order*, 35 FCC Rcd at 14321, para. 83. The Commission disagreed with those that argued that broad or general categories of equipment should not be included on the Covered List and rejected the view that the specified agencies must identify particular pieces or categories of equipment that posed an unacceptable risk. *USF Supply Chain Second Report and Order*, 35 FCC Rcd at 14322, para. 84.

[37] *USF Supply Chain Second Report and Order*, 35 FCC Rcd at 14322, para. 85.

[38] *Covered List Public Notice* at 2.

[39] *USF Supply Chain Second Report and Order*, 35 FCC Rcd at 14317-19, paras. 72-78.

[40] 47 CFR § 1.50002.

(1) Is produced or provided by any entity if, based exclusively on the following determinations, such equipment or service poses an unacceptable risk to the national security of the United States or the security and safety of United States persons:
   (i) A specific determination made by any executive branch interagency body with appropriate national security expertise, including the Federal Acquisition Security Council established under section 1222(a) of title 41, United States Code;
   (ii) specific determination made by the Department of Commerce pursuant to Executive Order No. 13873 (3 CFR, 2019 Comp., p 317); relating to securing the information and communications technology and services supply chain);
   (iii) Equipment or service being covered telecommunications equipment or services, as defined in section 889(f)(3) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232; 132 Stat. 1918); or
   (iv) A specific determination made by an appropriate national security agency;
(2) And is capable of:
   (i) Routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles;
   (ii) Causing the networks of a provider of advanced communications services to be disrupted remotely; or
   (iii) Otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons.[41]

17. The Commission defined certain terms associated with the Covered List. For purposes of § 1.50002(b)(1), the Commission interpreted "communications equipment and service" to include "any equipment or service used in fixed and mobile broadband networks that provides advanced communication service, provided the equipment or service includes or uses electronic components."[42] In making this interpretation, the Commission determined that all equipment or services that include or use electronic components can be reasonably considered essential to broadband networks, and believed that the definition will provide a bright-line rule that will ease regulatory compliance and administrability.[43] It interpreted equipment or services "capable of" the specified functions in § 1.50002(b)(2)(i)-(iii) as including equipment or service that can possibly perform these functions, even if the subject or equipment is not ordinarily used to perform the specified functions.[44] Finally, the Commission interpreted "advanced communications service" to mean high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology with connection speeds of at least 200 kbps in either direction.[45]

18. As noted above, the Secure Networks Act prohibited the use of any Federal subsidy made available through a program administered by the Commission that provides funds used for the capital expenditures necessary for the provision of advanced communications service, including all of the USF programs, to purchase, rent, lease, or otherwise obtain, or maintain "covered" communications equipment or services and directed the Commission to establish a reimbursement program to make reimbursements

[41] 47 CFR § 1.50002.

[42] *USF Supply Chain Second Report and Order*, 35 FCC Rcd at 14309, para. 52; 47 CFR § 1.50001(c).

[43] *USF Supply Chain Second Report and Order*, 35 FCC Rcd at 14309, para. 52. *See also id.* at 14309-10, paras. 53-54 (rejecting more narrow interpretations).

[44] *USF Supply Chain Second Report and Order*, 35 FCC Rcd at 14322-23, para. 86.

[45] *USF Supply Chain Second Report and Order*, 35 FCC Rcd at 14310-11, para. 55 (noting that this interpretation had unanimous support in the record and is consistent with the Commission's historic interpretation of section 706); 47 CFR § 1.50001(a).

to providers of advanced communications services to remove and replace "covered" equipment and services pursuant to an application process through which providers would obtain reimbursement.[46] In the *Supply Chain Secord Report and Order*, the Commission established this application process in section 1.50004 of its new rules.[47] Among other things, applicants are required to certify not only that they have developed a plan for permanent removal and replacement of "covered" communications equipment and services, but also that they will consult and consider the standards, guidelines, and best practices set forth in the cybersecurity framework developed by the National Institute of Standards and Technology in developing and tailoring the risk management.[48]

19. *Recent Executive Branch Actions*. On September 1, 2020, the Federal Acquisition Security Council issued an interim final rule to "standardize processes and procedures for submission and dissemination of supply chain information" and "facilitate the operations of a Supply Chain Risk Management Task Force under the [Council]."[49] It also provided the "criteria and procedures by which the [Council] will evaluate supply chain risk."[50] On January 19, 2021, the Commerce Department released an interim final rule with regard to Executive Order 13873, which gave the Secretary of Commerce authority to prohibit transactions of information and communications technology or services when, among other things, the transaction would pose undue risks to U.S. critical infrastructure or national security.[51]

20. On February 24, 2021, the President issued Executive Order 14017, which reiterates the importance of securing United States' supply chains from cyberattacks and other threats to national security. The President affirmed that the "United States needs resilient, diverse, and secure supply chains to ensure our economic prosperity and national security."[52] Noting that "close cooperation on resilient supply chains with allies and partners who share our values will foster collective economic and national security," this Order directs Executive Branch agencies to produce reports within 100 days to identify risks and recommendations for how to address those risks in the supply chains for various products – including semiconductors and rare earth elements, both of which are vital to modern communications technologies.[53] The Order also directs these agencies to produce reports within one year on the supply chains for specific sectors and subsectors, such as information and communications technologies (ICT), "including the industrial base for the development of ICT software, data, and associated services."[54]

---

[46] Secure Networks Act § 4(a).

[47] *USF Supply Chain Second Report and Order*, 35 FCC Rcd at 14334, para. 116; 47 CFR § 1.50004.

[48] Secure Networks Act § 4(d)(4). *See* Nat'l Inst. of Standards & Tech., *Cybersecurity Framework: New to Framework* (last updated Sept. 23, 2020), https://www.nist.gov/cyberframework/new-framework. This framework is "voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk." Nat'l Inst. of Standards & Tech., *Cybersecurity Framework: New to Framework*. NIST also has developed a Cybersecurity for the Internet of Things (IoT) program, which "supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed." Nat'l Inst. of Standards & Tech., *NIST Cybersecurity for IoT Program* (last updated Mar. 19, 2021), https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

[49] Office of Management and Budget, Federal Acquisition Supply Chain Security Act, 85 Fed. Reg. 54263 (Sept. 1, 2020).

[50] *Id.*

[51] https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain.

[52] Exec. Order No. 14017, 86 Fed. Reg. 11849, Executive Order on America's Supply Chains (Feb. 24, 2021), https://www.govinfo.gov/content/pkg/FR-2021-03-01/pdf/2021-04280.pdf.

[53] *Id.*

[54] *Id.* We note that since the Commission is an independent agency, it is not included within the scope of this Order.

21. On May 12, 2021, the President issued Executive Order 14028, which seeks to improve the nation's cybersecurity in various ways.[55] The Order begins by emphasizing that the United States "faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, private sector, and ultimately the American people's security and privacy."[56] Among other things, this Order directs the Secretary of Commerce to work through the Director of NIST to "initiate pilot programs informed by existing consumer product labeling programs to educate the public on the security capabilities of Internet-of-Things (IoT) devices and software development practices, and … consider ways to incentivize manufacturers and developers to participate in these programs."[57] This process will take place over the course of the next 12 months, in coordination with the Chair of the Federal Trade Commission and representatives from other agencies as deemed appropriate by the Director of NIST,[58] ultimately resulting in a report to the President reviewing the progress made and any "additional steps needed to secure the software supply chain."[59]

22. *March 2021 Publication of Covered List Specifying "Covered" Equipment and Services.* On March 21, 2021, the Public Safety and Homeland Security Bureau (PSHSB) published a list of "covered" communications equipment and services (Covered List) that are deemed to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons.[60] Pursuant to section 1.50002 of the Commission's rules, this Covered List identified certain equipment and services produced or provided by certain entities — specifically Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company — and their respective subsidiaries and/or affiliates.[61] The Commission tasked PSHSB with ongoing responsibilities for monitoring the status of the determinations and periodically updating the Covered List to address changes as appropriate.[62]

B. The Commission's Equipment Authorization Program

23. The Commission's equipment authorization rules play a critical role in enabling the Commission to carry out its responsibilities under the Communications Act. Under Section 302 of the Communications Act, the Commission is authorized to make reasonable regulations governing the interference potential of devices that emit radiofrequency (RF) energy and that can cause harmful interference to radio communications.[63] The purpose of the equipment authorization rules also is to promote efficient use of the radio spectrum and carry out various responsibilities associated with certain treaties and international regulations.[64] The Commission uses the equipment authorization program, codified in part 2 of our rules, to ensure that RF devices in the United States comply with the Commission's technical and equipment authorization requirements before they can be marketed in or

[55] Exec. Order No. 14028, Executive Order on Improving the Nation's Cybersecurity, 86 Fed. Reg. 26633 (May 17, 2021).

[56] *Id.* 86 Fed. Reg. at 26633, Section 1.

[57] *Id.* at 26640, Section 4(s).

[58] *Id.* at 26640-41, Section 4(t)-(w).

[59] *Id*. at 26641, Section 4(x).

[60] *Covered List Public Notice*; *see* 47 CFR §1.50002.

[61] 47 CFR § 1.50002; *see* Secure Networks Act § 2.

[62] 47 CFR § 1.50002. If the Covered List is not updated within one year, PSHSB will issue a public notice indicating that no updates were necessary during such period. *Id.*

[63] 47 U.S.C. § 302. Section 302(b) states that "[n]o person shall manufacture, import, sell, offer for sale, or ship devices or home electronic equipment and systems, or use devices, which fail to comply with regulations promulgated pursuant to this section."

[64] 47 CFR § 2.901.

imported to the United States.[65] The Commission's part 2 rules not only minimize the potential for harmful interference, but also ensure that those devices comply with the rules that address other policy objectives – such as human RF exposure limits,[66] hearing aid compatibility with mobile handsets,[67] and the Anti-Drug Abuse Act of 1988 (rule section 2.911(d)(2)).[68]

24. From the outset, the equipment authorization program has been tied to our efforts to ensure that RF devices imported to or marketed within the United States comply with the Commission's technical requirements. In December 1975, the Commission amended its rules with respect to the importation of certain electronic equipment, setting out the conditions under which RF devices and subassemblies of RF devices capable of causing harmful interference to radio communications may be imported into the United States.[69] Specifically, the Commission adopted a new subpart K to part 2, which stated, in part, regarding RF equipment: "In addition to the technical standards, the rules governing the service may require that such equipment receive an equipment authorization from the Commission as a prerequisite for marketing and importing this equipment into the U.S.A."[70] Subpart K has been modified in other proceedings over the past 45 years, but that sentence remains as a foundation for that subpart.[71] In 1998, the Commission eliminated two of the five categories of equipment authorization and relaxed the authorization procedures for devices that had a good history of compliance, allowing many consumer electronic devices to be authorized using self-approval procedures.[72] Later that year, the Commission approved the use of Telecommunications Certification Bodies (TCBs) to issue grants of Certification for certain RF devices in lieu of traditional grants being issued by the Commission. The creation of TCBs allowed the Commission to implement Mutual Recognition Agreements with the European Union, the Asia-Pacific Economic Cooperation, and other foreign trade partners.[73] In 2014, the Commission updated

---

[65] *See* 47 CFR part 2 Subpart I, §§ 2.801 *et seq*. (Marketing of Radio Frequency Devices); part 2 Subpart J, §§ 2.901 *et seq*. (Equipment Authorization Procedures); part 2 Subpart K, §§ 2.1201 *et seq*. (Importation of Devices Capable of Causing Harmful Interference). The Office of Engineering and Technology (OET) administers day-to-day operation of the equipment authorization program. *See* 47 CFR § 0.241(b). OET's Laboratory Division maintains a webpage devoted to the equipment authorization program. *See* the FCC's, Equipment Authorization Approval Guide, https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization.

[66] *See* 47 CFR §§ 2.1091, 2.1093.

[67] *See* 47 CFR § 20.19.

[68] *See* 47 CFR § 2.911(d)(2); *see also Amendment of Part 1 of the Commission's Rules to Implement Section 5301 of the Anti-Drug Abuse Act of 1988*, Gen. Docket No. 90-312, Report and Order, 6 FCC Rcd 7551 (1991) (*ADAA Report and Order*). The ADAA required any entity receiving a "federal benefit" to certify compliance with ADAA requirements. In its decision implementing the ADAA, the Commission applied the definition of "license" found in the Administrative Procedure Act (APA) to determine the scope of the term "license" as used in 47 U.S.C. section 5301 of the ADAA, and thus to define the scope of federal benefits. The APA defines "license" as including "the whole or part of an agency permit, certificate, approval, registration, charter, membership, statutory exemption or other form of permission." (5 U.S.C. § 551(8)). The *ADAA Report and Order* found that a wide range of Commission-regulated entities in various services must certify compliance with ADAA requirements.

[69] *See Amendment of Part 2 With Respect to Importation of Certain Electronic Equipment*, Docket No. 20194, Report and Order, 59 F.C.C.2d 1083 (1976).

[70] Id. at 1089, Appendix A at § 2.1201(a).

[71] 47 CFR § 2.1201(a).

[72] *See Streamlined Equipment Authorization Process for Radio Frequency Equipment*, ET Docket No. 97-94, Report and Order, 13 FCC Rcd 11415 (1998).

[73] See *1998 Biennial Regulatory Review — Amendment of Parts 2, 25 and 68 of the Commission's Rules to Further Streamline the Equipment Authorization Process for Radio Frequency Equipment, Modify the Equipment Authorization Process for Telephone Terminal Equipment, Implement Mutual Recognition Agreements and Begin Implementation of the Global Mobile Personal Communications by Satellite (GMPCS) Arrangements*, GEN Docket

(continued….)

its RF equipment authorization program by delegating the processing of all certification application to TCBs.[74]

25. In recent years, the Commission has taken steps to streamline the equipment authorization approval processes. As we recently discussed, the rapid and widespread deployment of RF devices has enabled the communications sector to drive innovation, promote economic growth, and become integral to nearly all aspects of modern life.[75] The Commission's equipment authorization program is essential to ensuring that the communications equipment Americans rely on every day, such as their cellphones and Wi-Fi devices, comply with the Commission's technical rules.[76] As we further noted, the number of devices now being authorized has expanded into the millions, RF equipment supply chains have become increasingly global, and manufacturers are under growing pressure to shorten the time it takes to bring new products to market.[77]

26. The last significant additions to the equipment authorization regulatory framework were adopted in 2017. In the *2017 Equipment Authorization Order*, the Commission modernized certain rules to align the equipment authorization processes with the current state of RF device technology and the global marketplace by, among other things, codifying contemporary electronic labeling (e-label) practices, modifying importation procedures and filing requirements, and changing the rules governing how personal devices and those used in trade shows may be brought into the country.[78] The *2017 Equipment Authorization Order* was part of a comprehensive review of the equipment authorization procedures that the Commission initiated in 2015.[79]

27. The Commission's current rules provide two different approval procedures for equipment authorization — Certification of equipment and Supplier's Declaration of Conformity (SDoC).[80] As a general matter, for an RF device to be marketed or operated in the United States, it must have been authorized for use through one of these two processes. We note, however, that some RF equipment has been exempted from the need for an equipment authorization.[81]

28. *Certification of Equipment.* In the certification process, which is the required process for RF devices with the greatest potential to cause harm to consumers or other radio operations, an equipment authorization is issued by an FCC-recognized Telecommunication Certification Body (TCB).

No. 98-68, Report and Order, 13 FCC Rcd 24687 (1998).[74] *See Amendment of Parts 0, 1, 2, and 15 of the Commission's Rules Regarding Authorization of Radiofrequency Equipment*, ET Docket No. 13-44, Report and Order, 29 FCC Rcd 16335 (2014).

[74] *See Amendment of Parts 0, 1, 2, and 15 of the Commission's Rules Regarding Authorization of Radiofrequency Equipment*, ET Docket No. 13-44, Report and Order, 29 FCC Rcd 16335 (2014).

[75] *See, e.g., Allowing Earlier Equipment Marketing and Importation Opportunities*, ET Docket 20-382, Notice of Proposed Rulemaking, 35 FCC Rcd 14458 (2020).

[76] *Id.* at 14458, para. 1.

[77] *Id.* at 14459, para. 5.

[78] *Amendment of Parts 0, 1, 2, 15 and 18 of the Commission's Rules regarding Authorization of Radiofrequency Equipment*, ET Docket No. 15-170, First Report and Order, 32 FCC Rcd 8746 (2017) (*2017 Equipment Authorization Order*).

[79] *See Amendment of Parts 0, 1, 2, 15, and 18 of the Commission's Rules regarding Authorization of Radiofrequency Equipment*, ET Docket No. 15-170, Notice of Proposed Rulemaking, 30 FCC Rcd 7725 (2015) (*2015 Equipment Authorization Notice*).

[80] *See, e.g., 2017 Equipment Authorization Order,* 30 FCC Rcd at 14459, para. 6.

[81] *See, e.g.*, 47 CFR § 15.103.

Certification is required for transmitters[82] and some unintentional radiators.[83] Examples of this equipment include wireless provider base stations and most transmitters in the associated services (e.g., CMRS), Wi-Fi access points routers, wireless Wi-Fi business solutions, home cable set-top boxes with Wi-Fi, laptops, tablets, intelligent home devices, and most wireless consumer equipment. Through the certification process, applicants file applications containing certain specified information required under the Commission's rules for that equipment – including various representations, written and signed certifications, and requisite information about the equipment (e.g., technical test data).[84] The TCB makes a determination as to whether to grant an equipment authorization based on evaluation of the supporting documentation and test data submitted to the TCB.[85] In this process, the Commission, through its Office of Engineering and Technology (OET), has general oversight of the certification application process, and OET provides guidance to TCBs via its knowledge database system (KDB).[86] Applications that involve certain categories of equipment or types of testing require a TCB to obtain "pre-approval guidance" from the Commission before the application may be approved.[87] If the TCB makes a determination to grant an equipment certification, information about this authorization is posted on a Commission-maintained public database.[88]

29. The part 2 rules also include various provisions that help ensure the integrity of the equipment authorization process. The Commission is authorized to dismiss or deny an application where that application in not in accordance with Commission requirements[89] or the Commission is unable to make the finding that grant of the application would serve the public interest.[90] The rules also provide that the TCB or Commission may set aside a grant of certification within 30 days if it is determined that such authorization does not comply with necessary requirements.[91] The rules also require the TCB to perform "post market surveillance" of equipment that has been certified, with guidance from OET, as may be appropriate.[92] Revocation of an existing equipment authorization is also authorized for certain specified reasons (including for false statements and representations in the application and other reasons).[93]

30. *Supplier's Declaration of Conformity (SDoC).* The Supplier's Declaration of Conformity (SDoC) process is available with respect to certain types of RF devices that have less potential to cause

[82] 47 CFR 2.907.

[83] 47 CFR § 15.101.

[84] *See* 47 CFR §§ 2.907 (Certification), 2.911-926 (Applications), 2.960-964 (Telecommunications Certification Bodies), 2.1031-1060 (Certification).

[85] *See* 47 CFR § 2.907(a). Testing associated with Certification must be performed by an FCC-recognized accredited testing laboratory, 47 CFR § 2.948(e).

[86] *See, e.g.*, KDB Publication Number: 641163: TCB Program Roles and Responsibilities, https://apps.fcc.gov/oetcf/kdb/forms/FTSSearchResultPage.cfm?id=44683&switch=P. The Knowledge Database (KDB) is an OET online database containing policies, procedures, and answers to common equipment authorization questions. It is available at www.fcc.gov/labhelp. It also provides a means to submit specific equipment authorization questions directly to OET Lab staff.

[87] 47 CFR § 2.964.

[88] 47 CFR § 2.941.

[89] 47 CFR §§ 2.917, 2.919.

[90] 47 CFR §§ 2.915(a), 2.918.

[91] 47 CFR § 2.962(f)(6).

[92] 47 CFR § 2.962(g).

[93] 47 CFR § 2.939.

interference. The SDoC procedure requires the party responsible for compliance ("responsible party") to make the necessary measurements and complete other procedures found acceptable to the Commission to ensure that the particular equipment complies with the appropriate technical standards for that device.[94] For example, SDoC is an option[95] for certain devices that may be operated under part 15 of the Commission's rules without a license,[96] specific part 18 consumer industrial, scientific, and medical (ISM) equipment,[97] and some transmitters operating in licensed services.[98] The information provided, at the time of marketing or importation, with devices subject to SDoC must include a compliance statement that lists a U.S.-based responsible party.[99] The responsible party for equipment subject to the SDoC process could include the equipment manufacturer, the assembler (if the equipment is assembled from individual component parts and the resulting system is subject to authorization), or the importer (if the equipment by itself or the assembled system is subject to authorization).[100] The SDoC signifies that the responsible party has determined that the equipment has been shown to comply with the applicable technical standards.[101] Responsible parties are required to retain records on the equipment that demonstrate the equipment's compliance with the Commission's applicable requirements for that equipment.[102] The Commission can specifically request that such information on particular equipment be provided to the Commission.[103]

31. *Equipment exempted from needing an equipment authorization.* Section 15.103 of our rules exempts certain RF devices from an equipment authorization.[104] This exemption pertains to specified digital devices contained in several types of products that generate such low levels of RF emission that they have virtually no potential for causing harmful interference to with the authorized radio services.[105] Exempt devices include those that are used exclusively in the following – transportation vehicles, including motor vehicles and aircraft; as an electronic control or power system utilized by a public utility or in an industrial plant; as industrial, commercial, or medical test equipment; and in an appliance. It also excludes devices that are used for specialized medical use, have a very low power

---

[94] *See* 47 CFR §§ 2.906 ("Supplier's Declaration of Conformity"); 2.909 ("Responsible Parties"); 2.938 ("Retention of records"); 2.945 ("Submission of equipment for testing and equipment records"); 2.1071-1077 ("Supplier's Declaration of Conformity").

[95] If desired, the responsible party for a device may choose to file an application for certification in lieu of completing the SDoC process. *See* 47 CFR § 2.906(c).

[96] 47 CFR § 15.101.

[97] 47 CFR § 18.203.

[98] Including, for example, certain broadcast and fixed microwave service transmitters, 47 CFR §§ 73.1660 and 101.139, respectively.

[99] 47 CFR § 2.1077.

[100] 47 CFR § 2.909(b)(1)-(2).

[101] 47 CFR § 2.1072(a).

[102] 47 CFR § 2.938.

[103] 47 CFR §§ 2.906(a); 2.945(b)(1) (Commission may request that the responsible party or any other party marketing the equipment submit a sample); 2.945(c) (upon request by the Commission, each responsible party shall submit copies of records required under the Commission's rules, including -- the original design drawings and specification; procedures for inspection and testing; test results; actual date of testing; name of the test lab, company, or individual performing the testing; description of the equipment; and/or the "compliance information" required under the rules). *See* 47 CFR § 2.1077 (Compliance information).

[104] 47 CFR § 15.103.

[105] *Revision of Part 15 of the Rules Regarding the Operation of Radio Frequency Devices without an Individual License*, GN Docket No. 87-389, Notice of Proposed Rulemaking, 2 FCC Rcd 6135, 6140, para. 39 (1987).

consumption (i.e., not exceeding 6 nW), are used in joystick or similar controllers, or are devices that operate on low frequencies (i.e., below 1.705 MHz) and which do not operate from the AC power lines or contain provisions for operation while connected to the AC power lines.[106] Additionally, most satellite transmitters[107] and most amateur radio equipment[108] do not require an equipment authorization and certain specified equipment regulated under other rule parts also does not require equipment authorization.

32. *Existing part 2 rules and "covered" equipment on the Covered List.* At this time, the Commission's current equipment authorization rules do not include specific provisions addressing the "covered" equipment on the Covered List.

C. Certifications in Commission Competitive Bidding and Prospective Safeguards in the Public Interest

33. The Commission uses competitive bidding to determine which among multiple applicants with mutually exclusive applications for a license may file a full application for the license.[109] This process furthers multiple public interest objectives, including the development and rapid deployment of new technologies, products, and services without delays and the efficient and intensive use of the electromagnetic spectrum.[110]

34. Congress gave the Commission the authority to require such information and assurances from applicants to participate in competitive bidding as is necessary to demonstrate that their application is acceptable.[111] Pursuant to this authority, the Commission has required each applicant to participate in competitive bidding to make various certifications.[112] The substance of these required certifications cover a range of public interest concerns related to the conduct of competitive bidding and the national security interest in precluding some parties from becoming licensed through competitive bidding.[113] Parties unable to make the required certifications have their applications to participate dismissed.[114]

III. DISCUSSION

35. In this Notice of Proposed Rulemaking and Notice of Inquiry we examine our rules relating to equipment authorization and participation in Commission auctions to help advance the Commission's goal of protecting national security and public safety. This proceeding builds on other actions the Commission recently has taken to protect and secure our nation's communications systems.

36. As described above, in other proceedings over the last three years, the Commission has taken several actions to prevent use of equipment and services that pose an unacceptable risk to our

[106] *Id*.

[107] Satellite communications are regulated under part 25 of the Commission's rules. Subpart B of that part specifies general rules and subpart D specifies technical standards for satellite transmitters, but equipment authorization is not specified, except for portable earth-station transceivers. *See* 47 CFR § 25.129.

[108] The Amateur radio service is regulated under part 97 of the Commission's rules. Subpart D of that part specifies technical standards for equipment, but only external RF power amplifiers are subject to equipment authorization; *see* 47 CFR § 97.315.

[109] *See* 47 U.S.C. § 309(j)(1).

[110] *See* 47 U.S.C. § 309(j)(3)(A) and (D).

[111] *See* 47 U.S.C. § 309(j)(5).

[112] 47 CFR § 1.2105(a)(2)(iv)-(xiii).

[113] *See* 47 CFR § 1.2105(a)(2)(ix) (regarding joint bidding arrangements) and (xiii) (regarding bars against participation in certain auctions based on national security).

[114] 47 CFR § 1.2105(b)(1).

nation's communications networks.[115] In June 2020, The Public Safety and Homeland Security Bureau designated Huawei and ZTE as national security threats to the integrity of communications networks, prohibiting the use of Universal Service Fund support to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by Huawei and ZTE.[116] Most recently, the Public Safety and Homeland Security Bureau (PSHSB), as required by the December 2020 *USF Supply Chain Second Report and Order*,[117] published the Covered List, which identifies "covered" equipment and services that pose an unacceptable risk to national security or to the security and safety of U.S. persons.[118] The PSHSB will continue to update that list as appropriate. Although the Commission, through PSHSB publishes and updates the Covered List, the equipment and services included on the list are identified by specific external sources enumerated in the Secure Networks Act.[119]

37. This Covered List identifies communications equipment and services that pose an unacceptable risk to the national security of the United States or the security and safety of United States persons. The Commission is required to include communications equipment and services on the list based exclusively on determinations made by Congress and by other U.S. government agencies.[120] Currently, the list includes equipment and services produced or provided by five entities:

- "Telecommunications equipment produced or provided by" Huawei Technologies Company or ZTE Corporation, or their respective subsidiaries and affiliates, "including telecommunications or video surveillance services produced or provided by such [entities] or using such equipment;" and
- "Video surveillance and telecommunications equipment produced or provided by" Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company, or their respective subsidiaries and affiliates, "to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services produced or provided by such [entities] or using such equipment."[121]

Under the Secure Networks Act and the Commission's new rule, part 1, subpart DD, inclusion of equipment and services on the Covered List precludes the use of federal subsidy funds – e.g., funds from the Commission's Universal Service Programs – to obtain or maintain such equipment or services.[122]

38. The Notice of Proposed Rulemaking seeks comment on various steps that the

[115] See Section II.A, above (discussion of recent Commission proceedings and actions).

[116] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation*, PS Docket No. 19-351, Order, 35 FCC Rcd 6604 (PSHSB 2020) (*Huawei Designation Order*); *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – ZTE Designation*, PS Docket No. 19-352, Order, 35 FCC Rcd 6633 (PSHSB 2020) (*ZTE Designation Order*).

[117] *USF Supply Chain Second Report and Order*, 35 FCC Rcd 14284.

[118] *Covered List Public Notice*; *see* 47 CFR § 1.50002.

[119] 47 CFR § 1.50002(b)(1)(i)-(iv).

[120] Secure Networks Act, § 2(c) (47 U.S.C. § 1601(c)).

[121] *Covered List Public Notice* at 3. As noted in this Public Notice, where equipment or services on the list are identified by category, such category should be construed to include only equipment or services capable of the functions outlined in sections 2(b)(2)(A), (B), or (C) of the Secure Networks Act. 47 U.S.C. § 1601(b)(2)(A)-(C).

[122] 47 U.S.C. § 1602; 47 CFR § 1.50000 *et seq.*; *see Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Declaratory Ruling and Second Further Notice of Proposed Rulemaking, 35 FCC Rcd 7821, 7825-28, paras. 16-22 (2020).

Commission could take in its equipment authorization program, as well as its competitive bidding program, to reduce threats posed to our nation's communications system by "covered" equipment and services on the Covered List. In the Notice concerning our equipment authorization rules and processes, we propose revisions to the Commission's equipment authorization rules and procedures under part 2 to prohibit authorization of any "covered" equipment on the Covered List. We also seek comment on whether the Commission should revoke equipment authorizations of "covered" equipment, and if so under what conditions and procedures. In addition, we include in the Notice questions concerning possible revisions to the Commission's competitive bidding procedures that could address certain concerns related to "covered" equipment and services. Notably, the Commission must "periodically update the list . . . to address changes in [external] determinations . . . [and] shall monitor the making and reversing of determinations . . . in order to place additional communications equipment or services on the list . . . or to remove communications equipment and services from such list."[123] If one of the enumerated sources named in the Secure Networks Act modifies or deletes a determination, PSHSB will do the same and modify the Covered List accordingly.[124] We seek comment on how future updates to the Covered List should affect our proposals in this Notice.

39. Finally, we adopt a Notice of Inquiry seeking comment on other actions that the Commission should consider taking within the context of equipment authorizations that would serve to protect our nation's communications networks and incentivize manufacturers to develop and produce equipment that is more resilient and secure.

A. Notice of Proposed Rulemaking

1. Equipment Authorization Rules and Procedures

40. In this Notice, we propose revisions to the Commission's equipment authorization rules and processes to prohibit authorization of any "covered" equipment on the Covered List. This prohibition would apply to "covered" equipment on the Covered List maintained and updated by PSHSB. We also seek comment on whether our rules concerning equipment currently exempted from the equipment authorization requirement should be revised to ensure that any "covered" equipment cannot qualify for such exemption. We also seek comment on whether we should revoke any of the authorizations that have been previously granted for "covered" equipment on the Covered List, and if so, which ones and through what procedures. Finally, we seek comment on new certifications for applicants that wish to participate in Commission auctions that would further address the risks posed by companies that the Commission has designated as posing a national security threat to the integrity of communications networks and the communications supply chain.

a. Equipment Authorization Rules Under Part 2

(i) General Provisions of Subpart J

41. The Commission's rules and procedures set forth in part 2 of the Commission's rules include requirements and processes for equipment marketing,[125] authorization,[126] and importation.[127] We propose to adopt a new subsection 2.903, as part of the "General Provisions" of subpart J, to provide general guidance regarding the prohibition on equipment authorizations with respect to communications

[123] Secure Networks Act § 2d(1)-(2); *see also* 47 CFR § 1.50003.

[124] *See* 47 CFR § 1.50003(b) (if a determination regarding covered communications equipment or service on the Covered List is reversed or modified, directing PSHSB to remove from or modify the entry of such equipment or service on the Covered List, except if any of the sources identified in 47 CFR § 1.50002(b)(1)(i)-(iv) maintains a determination supporting inclusion of such equipment or service on the Covered List).

[125] 47 CFR §§ 2.801 *et seq.*

[126] 47 CFR §§ 2.901 *et seq.*

[127] 47 CFR §§ 2.1201 *et seq.*

equipment on the Covered List.

> § 2.903 Prohibition on equipment authorization of equipment on the Covered List.
>
> Any equipment on the Covered List, as defined in § 1.50002 of this chapter, is prohibited from obtaining an equipment authorization under this subpart. This includes:
>
> (a) Equipment subject to certification procedures: Telecommunication Certification Bodies and the Federal Communications Commission are prohibited from issuing a certification under this subpart for any equipment on the Covered List; and
>
> (b) Equipment subject to Supplier's Declaration of Conformity procedures: Responsible parties, as defined in § 2.909 of this part, associated with the Supplier's Declaration of Conformity are prohibited from issuing a Supplier's Declaration of Conformity for any equipment on the Covered List.

In proposing this new rule section, we seek to establish a clear prohibition on authorization of any "covered" equipment in our equipment authorization processes regardless of the process to which that equipment is subject. We seek comment on this proposed rule. Is this rule sufficient to prohibit any such equipment on the Covered List from being authorized for use in the United States? What modifications or clarifications are needed to this proposed language to ensure that the rule is clear as to its scope and effect and attains results commensurate with its purpose to protect national security? Are there additional provisions that should be included here to more fully capture the scope of our proposed prohibition?[128]

42. We note that if the Commission were to adopt this proposal to revise the Commission's subpart J equipment authorization rules to prohibit any further authorization of "covered" equipment through the certification or SDoC processes, this decision would also serve to prohibit the marketing of such equipment that would now be prohibited from authorization under subpart I of the Commission's part 2 rules (Marketing of Radio-Frequency Devices)[129] and importation of equipment under subpart K (Importation of Devices Capable of Causing Harmful Interference) of the Commission's part 2 rules. Section 2.803(b) of subpart I only permits persons to import or market RF devices that are subject to authorization under either the certification or SDoC process, as set forth in the Commission's subpart J rules, once those devices have been authorized,[130] unless an exception applies.[131] Similarly, our proposed revisions in subpart J, above, also would serve to prohibit importing or marketing of "covered" equipment if it is subject to authorization through either the certification or SDoC process in subpart J and has not been authorized, per sections 2.1201(a) and 2.1204(a).[132] We seek comment on whether we need to revise or provide clarification with regard to how our proposed prohibition of authorization of "covered"

[128] We note that provisions in various rule parts exempt certain types or classes of equipment from certification or other approval requirements and seek comment on whether that equipment need also be included here or whether specific provisions need to be placed in those rule parts to ensure that covered equipment cannot be used. For example, devices described in section 15.103 are not subject to any equipment authorization procedures. Similarly, section 90.203 generally requires all devices that operate under that part to be certified but contains provisions that exempts certain devices from that requirement. Under part 25, only portable earth station transceivers are subject to equipment certification procedures; all other Part 25 equipment is exempt for equipment authorization procedures. *See* 47 CFR § 25.129. Also, under Part 97 only external power amplifiers used in the Amateur Radio Service are required to obtain equipment certification; all other equipment is exempt from equipment authorization procedures. *See* 47 CFR § 97.315.

[129] 47 CFR §§ 2.801 *et seq.*

[130] 47 CFR § 2.803(b) (concerning Part 2 Subpart I rules, "Marketing of Radio-Frequency Devices").

[131] 47 CFR § 2.803(c) (listing the exceptions to the general rule of section 2.803(b)).

[132] 47 CFR §§ 2.1201(a), 2.1204(a) (concerning part 2, subpart K rules, "Importation of Devices Capable of Causing Harmful Interference").

equipment affects the implementation of the Commission's rules in either subpart I or subpart K. Would the general prohibition we propose for equipment subject to certification and SDoC make any changes to subparts I or K unnecessary? If not, what changes are needed to our rules in those subparts?

43. Below, we seek comment on other revisions that the Commission should make regarding either certification issued by a TCB or Supplier's Declaration of Conformity (SDoC). We discuss and seek comment on how our proposed rule should be implemented with respect to each of these processes, and whether other rule revisions or clarifications are appropriate. While the vast majority of RF devices are subject to either certification or SDoC under the rules in subpart J, there is a limited category of devices that are exempt from these authorization processes. We also seek comment on how best to address this equipment.

(ii) Certification Rules

44. *Background.* As described in brief above, under the Commission's equipment authorization rules, certain radiofrequency devices that have the greatest potential to cause harmful interference to radio services, must be processed through the equipment certification procedures. Certification generally is required for transmitters[133] as well as some unintentional radiators.[134] Examples of equipment include mobile phones, wireless provider base stations, point-to-point and point-to-multipoint microwave stations, land mobile, maritime and aviation radios, Wi-Fi access points and routers home cable set-top boxes with Wi-Fi , as well as most wireless consumer equipment (e.g., tablets, smartwatches and smart home automation devices). Applicants are required to file with an FCC-recognized Telecommunication Certification Body (TCB) applications containing specified information.[135] Each applicant is required to provide the TCB with all pertinent information as required by the Commission's rules.[136] These requirements generally specify the information necessary to document compliance with the testing requirements that broadly apply to RF devices used under authority of the Commission, including devices used under licensed radio services and devices used on an unlicensed basis.[137] Additional application information is required to demonstrate compliance with specific technical requirements in particular service rules (e.g., that antennas on certain unlicensed part 15 devices are not detachable[138] or that certain part 90 private land mobile transmitters meet required efficiency standards[139]) or other broadly applicable policy-related Commission requirements (e.g., compliance with the Anti-Drug Abuse Act[140]). By signing the application for equipment authorization (FCC Form 731), each applicant attests that the information provided in all statements and exhibits pertaining to that particular equipment are true and correct.[141] The TCB then makes a determination as to

[133] *See e.g.*, 47 CFR §§ 25.129, 27.51, 95.361.

[134] 47 CFR § 15.101.

[135] *See* 47 CFR §§ 2.907 (Certification), 2.911-926 (Applications), 2.960-964 (Telecommunication Certification Bodies), 2.1031-1060 (Certification).

[136] *See, e.g.*, 47 CFR §§ 2.911(d), 2.1033(a).

[137] *See, e.g.*, 47 CFR §§ 2.1033(b), 2.1033(c)(1)-(14).

[138] 47 CFR § 15.203.

[139] 47 CFR § 90.203(j).

[140] 47 CFR §§ 1.2002; 2.911(d)(2).

[141] *See* FCC Form 731, "Applicant/Agent Certification" section which states, "I certify that I am authorized to sign this application. All of the statements herein and the exhibits attached hereto, are true and correct to the best of my knowledge and belief. IN accepting a Grant of Equipment Authorization issued by the FCC as a result of the representations made in this application, the applicant is responsible for (1) labeling the equipment with the exact FCC ID specified in this application, (2) compliance statement labeling pursuant to the applicable rules, and (3) compliance of the equipment with the applicable technical rules. If the applicant is not the actual manufacturer of the (continued….)

whether to grant an equipment certification based on evaluation of the submitted documentation and test data.[142] The Commission, through OET, oversees the certification application process, and provides guidance to applicants, TCBs, and test labs through its pre-approval guidance (including its knowledge database system (KDB)) with regard to required testing and other information associated with certification approval procedures and processes.[143] Applications that involve new technology or for which there are no FCC-recognized test procedures require a TCB to obtain pre-approval guidance from the Commission before the application may be approved.[144] Once a TCB makes a determination, either on its own or after consultation with the Commission, to grant an equipment certification, information about that authorization is publicly announced "in a timely manner" through posting on the Commission-maintained Equipment Authorization System (EAS) database,[145] and referenced via unique FCC identifier (FCC ID).[146] Once this original certification is granted, the device is subject to rules that specify requirements: for modifying equipment,[147] marketing under or changing FCC ID,[148] and transferring ownership of an FCC ID.[149]

45. The Commission's part 2 rules also include various provisions that help ensure that equipment certifications comply with Commission requirements. The Commission is authorized to dismiss or deny an application where that application in not in accordance with Commission requirements[150] or the Commission is unable to make a finding that grant of the application would serve the public interest.[151] The rules also provide that the TCB or Commission may set aside a certification within 30 days of grant if it determines that the equipment does not comply with necessary requirements.[152] The rules also require the TCB to perform "post market surveillance" of equipment that has been certified, with guidance from OET, as may be appropriate.[153] Revocation of an existing equipment authorization is also authorized for various reasons, including for false statements and representations in the application. And an authorization may be withdrawn if the Commission changes its

---

equipment, appropriate arrangements have been made with the manufacturer to ensure that production units of this equipment will continue to comply with the FCC's technical requirements.

Authorizing an agent to sign this application, is done solely at the applicant's discretion; however, the applicant remains responsible for all statements in this application.

If an agent has signed this application on behalf of the applicant, a written letter of authorization which includes information to enable the agent to respond to the above section 5301 (Anti-Drug Abuse) Certification statement has been provided by the applicant. It is understood that the letter of authorization must be submitted to the FCC upon request, and that the FCC reserves the right to contact the applicant directly at any time."

[142] *See* 47 CFR § 2.907(a). Testing associated with Certification must be performed by an FCC-recognized accredited testing laboratory, 47 CFR § 2.948(e).

[143] *See, e.g.,* §§ 2.947(a)(3) and 2.1093(d)(2) which state that advisory information regarding measurement procedures can be found in the KDB.

[144] 47 CFR § 2.964.

[145] 47 CFR § 2.941. Certified devices are associated with a unique FCC Identification Number.

[146] 47 CFR §§ 2.925, 2.926.

[147] 47 CFR §§ 2,962, 2.1043.

[148] 47 CFR §§ 2.924, 2.933

[149] 47 CFR § 2.929.

[150] 47 CFR § 2.917.

[151] 47 CFR §§ 2.915(a), 2.918.

[152] 47 CFR § 2.962(f)(6).

[153] 47 CFR § 2.962(g).

technical standards.[154]

46. *Discussion.* We propose certain additional revisions to the Commission's rules and processes regarding equipment certification. In proposing to revise our equipment certification rules, our goal is to design a process that efficiently and effectively prohibits authorization of "covered" equipment without delaying the authorization of innovative new equipment that benefits our lives.

47. We propose revising the equipment certification application procedures to include a new provision in section 2.911 that would require applicants to provide a written and signed attestation that, as of the date of the filing of the application, the equipment for which the applicant seeks certification is not "covered" equipment on the Covered List. Specifically, any applicant for certification would attest that no equipment (including component part) is comprised of any "covered" equipment, as identified on the current published list of "covered" equipment. This new provision also would cross-reference section 1.50002 of the Commission's rules that pertain to the Covered List.[155] We seek comment on this proposal. We also invite comment on particular language that should be included in this attestation. For instance, to what extent should we consider basing this attestation language on the certifications that providers of advanced communications services must complete to receive a Federal subsidy made available through a program administered by the Commission that provides funds to be used for the capital expenditures necessary for the provision of advanced communications services?

48. Section 2.1033 discusses information that must be included in the application. We seek comment on whether there are revisions that the Commission should adopt in this rule provision that would further clarify our proposals regarding prohibition of the certification of any "covered" equipment. What information may be pertinent to assist the TCBs and the Commission in ensuring that applications do not seek certification of "covered" equipment? Should the Commission require that the applicant provide certain information that would help establish that the equipment is not "covered" equipment, to assist TCBs and the Commission in making determinations about whether to grant the application? For example, the Commission currently requires applicants to file block diagrams or schematic diagrams of their devices.[156] Should we also require a parts list noting the manufacturer of each part? If we were to adopt such a requirement, should it apply to all or only certain components? Which ones? How much additional burden, if any, would this place on applicants as compared to the current level of effort needed to prepare an equipment certification application?

49. We propose to direct OET to develop guidance for use by interested parties, including applicants and TCBs, regarding the Commission's proposed prohibition on certification of "covered" equipment. In particular, we propose to direct PSHSB, the Wireline Competition Bureau (WCB), the Wireless Telecommunications Bureau, and the International Bureau to assist OET in developing pre-approval guidance[157] that provides the necessary guidance that TCBs can use and should follow in implementing the proposed prohibition. PSHSB, which is tasked with publication of the Covered List, and has significant responsibilities and expertise regarding ensuring that our nation's public safety communications networks are secure, can lend important assistance by collaborating with OET to provide such guidance.[158] We seek comment on this proposal. We also seek comment on whether the current pre-

[154] 47 CFR § 2.939.

[155] 47 CFR § 1.50002 (Covered List).

[156] 47 CFR § 2.1033(b)(5).

[157] 47 CFR § 2.964 (Pre-approval guidance procedure for Telecommunications Certification Bodies).

[158] We note that with regard to the existing list of "covered" equipment is equipment produced or provided by Hytera Technologies Company, Hangzhou Hikvision Digital Technology, and Dahua Technology (and the subsidiaries and affiliates of these entities) to the extent that the equipment concerns video surveillance and telecommunications equipment associated with public safety, security of government facilities, physical security

(continued….)

approval guidance rule (or the use of KDBs) should be revised or clarified consistent with our goals in this proceeding.

50. As we have noted, following a TCB's grant of certification the Commission will post information on that grant "in a timely manner" on the Commission-maintained public EAS database.[159] As we have also noted, the TCB or Commission may set aside a grant of certification within 30 days of the grant date if it is determined that such authorization does not comply with necessary requirements or is not in the public interest.[160] Should we adopt procedures that ensure that posting of any grant is achieved in speedy fashion (e.g., within five business days of grant) to provide more time for review by the TCB or the Commission or for the public to bring possible material information to the attention of either the TCB or the Commission, that might warrant setting aside the grant? To what extent should interested parties, whether the public or government entities (e.g., other expert agencies) be invited to help inform the Commission as to whether particular equipment inadvertently received a grant by the TCB and is in fact (or might be) "covered" equipment such that the grant should be set aside? Should the Commission consider adopting any new procedures for gathering and considering information on potentially relevant concerns that the initial grant is not in the public interest and should be set aside? Should such procedures be limited to certain parties (e.g., expert agencies), or certain minimal showings required by those that seek to raise questions about the grant?[161]

51. Section 2.962(g) of our current rules expressly provides for "post-market surveillance" activities with respect to products that have been certified.[162] We propose to direct OET, in exercising its delegated authority, to provide TCBs with guidance on the kinds of post-market surveillance that should be conducted to help ensure that no equipment that subsequently has been authorized includes ""covered" equipment that has not been authorized. Here, we seek comment on whether revisions or clarifications to the post-market surveillance requirements should be adopted. Under existing rules, TCBs are required to conduct type testing of samples of product types that the TCBs have certified. OET has delegated authority to develop procedures that TCBs will use for performing such post-market surveillance, including the responsibility for publishing a document on the post-market surveillance requirements that will provide specific information such as the numbers and types of samples the TCBs must test. OET may also request that a grantee of equipment certification submit a sample directly to the TCB that performed the original certification for its evaluation. TCBs also may request samples directly from the grantee. If in this post-market surveillance the TCB determines that the product fails to comply with the technical regulation for that product, the TCB then notifies the grantee and the grantee must then describe actions taken to the correct the situation. The TCB provides a report of these actions to the Commission within 30 days.[163]

52. We also seek comment on how our rules should be implemented, or revised or clarified, to ensure that equipment users will not make modifications to existing equipment that would involve replacing equipment (in whole or part) with "covered" equipment. Should, for instance, the Commission revise or clarify its section 2.932 rules regarding modifications or the section 2.1043 provisions concerning "permissive changes," to promote our goals in this proceeding? We also note that section

surveillance infrastructure, other national security purposes. *Covered List Public Notice* at 3. PSHSB has important regulatory responsibilities and subject matter expertise on this type of equipment.

[159] 47 CFR § 2.941

[160] 47 CFR § 2.962(f)(6).

[161] As discussed below with regard to revocation of equipment authorizations, we propose that if the Commission were to determine, after this 30-day period, that an applicant made false statements in its application regarding "covered equipment," that authorization can be revoked. See discussion below, paragraph [__].

[162] 47 CFR § 2.962(g).

[163] *Id.* at 2.

2.929 of our equipment authorization rules includes provisions regarding changes in the name, address, ownership, or control of the grantee of an equipment authorization.[164] An equipment authorization may not be assigned, exchanged, or in any other way transferred to a second party, except as provided in this section.[165] Should we consider any revisions or clarifications about how these provisions apply in light of our proposals regarding prohibition on authorization of "covered" equipment? For example, should we prohibit the ownership or control of the certification for any equipment on the Covered List from being assigned, exchanged or transferred to another party?

53. Under our part 2 rules concerning equipment authorization, various provisions are included that help ensure that applicants and TCBs comply with their responsibilities related to the Commission's equipment authorization procedures set forth in part 2 Subpart J. We note, for instance, that pursuant to section 2.911(d)(1), applicants must provide a written and signed certification to the TCB that all statements in its request for equipment authorization are true and correct to the best of its knowledge and belief.[166] TCBs, which are subject to the accreditation process, must comply with all applicable responsibilities set forth in our part 2 rules for TCBs,[167] and if we were we to adopt our proposal would be obligated to prohibit the certification of any "covered" equipment. In reviewing the applications, TCBs would be required to dismiss any application should it become aware that an applicant has falsely asserted that its equipment (or components of the equipment) is not "covered" equipment. We seek comment on our implementation of these rules in the context of prohibiting certification of "covered" equipment, and any revisions or clarifications that may be appropriate to ensure that from this point forward applicants and TCB's comply with our proposed prohibition on authorization of "covered" equipment.

54. As discussed above, PSHSB will periodically publish updates to identify the "covered" equipment and services that are on the Covered List.[168] Under our proposals, we accordingly direct that OET expeditiously take all the appropriate steps (e.g., updating as necessary the precise certification that applicants must make that no newly identified "covered" equipment is associated with the application, as well as updating any pre-approval guidance, KDB, or other guidance) to reflect those updates, consistent with the rules and procedures that the Commission ultimately adopts regarding the certification rules in this proceeding. We invite comment on appropriate means for OET to include updates of the "covered" equipment in an expeditious fashion in ways that best ensure that applicants, TCBs, and other interested parties will comply with the prohibitions concerning this updated identification of "covered" equipment.

55. Finally, we seek comment on whether there are other rule revisions or clarifications to the equipment certification rules and processes that the Commission should make consistent with our goals to prohibit authorization of "covered" equipment. Commenters should explain their suggestions in sufficient detail, including the reasoning behind the suggestions and associated issues (e.g., implementation).

(iii) Supplier's Declaration of Conformity (SDoC) rules

56. *Background.* The Supplier's Declaration of Conformity (SDoC) process is available for many types of equipment that have less potential to cause RF interference. Under our rules, the types of equipment that may be processed pursuant to the SDoC procedures include fixed microwave transmitters (e.g., point-to-point or multipoint transmitter links as well as some links used by carriers and cable

[164] 47 CFR § 2.929.

[165] *Id.*

[166] 47 CFR § 2.911(d)(1). As we discuss below, false statements or representations are grounds for revocation of the equipment authorization. 47 CFR § 2.939(a)(1).

[167] 47 CFR § 2.962.

[168] *Covered List Public Notice* at 2.

operators) authorized under part 101, broadcast TV transmitters authorized under Parts 73 and 74, [discuss example of equipment] authorized under Parts 80 (Marine), [discuss example of equipment] authorized under part 87 (Aviation), and private land mobile radio services equipment [describe] and equipment associated with special services such as global maritime distress and safety system, aircraft locating beacons, ocean buoys), certain unlicensed equipment (e.g., business routers, firewalls, internet routers, internet appliances, wired surveillance cameras, business servers, workstations, Laptops, almost all enterprise network equipment, computers, alarm clocks) authorized under part 15, certain ISM equipment (e.g., those that use RF energy for heating or producing work) authorized under part 18. The SDoC process differs significantly from the certification process for equipment authorizations, and relies on determinations about the equipment made by the party responsible for compliance ("responsible party" as defined in the rules) as to whether the equipment "conforms" with the Commission's requirements. Using the more streamlined SDoC process for the equipment authorization is "optional" insofar as the responsible party may choose to apply for equipment certification through the equipment certification process even if SDoC is acceptable under our rules.[169]

57. In the SDoC process, the responsible party makes the necessary measurements and completes other procedures found acceptable to the Commission to ensure that the particular equipment complies with the appropriate technical standards for that device.[170] The information provided with devices subject to SDoC must include a compliance statement that lists a U.S.-based responsible party. As set forth in the rules, the responsible party for equipment subject to the SDoC process could include the equipment manufacturer, the assembler (if the equipment is assembled from individual component parts and the resulting system is subject to authorization), or the importer (if the equipment by itself or the assembled system is subject to authorization),[171] and could also include retailers and parties performing modification under certain circumstances.[172] The SDoC signifies that the responsible party has determined that the equipment has been shown to comply with the applicable technical standards.[173] Given the streamlined nature of this particular process, responsible parties are not typically required to submit to the Commission an equipment sample or representative data demonstrating compliance.[174] Also, while our rules require that the equipment authorized under the SDoC procedure must include a unique identifier, the equipment is not listed in a Commission equipment authorization database,[175] they are required to retain records on the equipment that demonstrate the equipment's compliance with the Commission's applicable requirements for that equipment.[176] The Commission can specifically request that the responsible parties provide such information on particular equipment to the Commission.[177]

---

[169] 47 CFR § 2.906(c).

[170] *See* 47 CFR §§ 2.906 ("Supplier's Declaration of Conformity"); 2.9391 ("Responsibilities"); 2.938 ("Retention of records"); 2.945 ("Submission of equipment for testing and equipment records"); 2.1071-1077 ("Supplier's Declaration of Conformity").

[171] 47 CFR § 2.909(b)(1)-(2).

[172] 47 CFR § 2.909(b)(3)-(4).

[173] 47 CFR § 2.1072(a).

[174] 47 CFR § 2.906(a).

[175] 47 CFR § 2.1074. The format of "unique identifier" is at the responsible party's discretion and has no correlation to a Commission established FCC ID.

[176] 47 CFR § 2.938.

[177] 47 CFR §§ 2.906(a); 2.945(b)(1) (Commission may request that the responsible party or any other party marketing the equipment submit a sample); 2.945(c) (upon request by the Commission, each responsible party shall submit copies of records required under the Commission's rules, including – the original design drawings and specification; procedures for inspection and testing; test results; actual date of testing; name of the test lab, company, (continued….)

58. *Discussion*. We propose that any equipment on the Covered List, can no longer be processed pursuant to the Commission's SDoC processes, and any "covered" equipment of any of these entities would have to be processed pursuant to the Commission's certification rules and processes as proposed above. Accordingly, responsible parties would be prohibited altogether from issuing the SDoC process with respect to any "covered" equipment and such equipment would be prohibited from obtaining equipment authorization through the SDoC process. That is not to say that all "covered" equipment currently subject to the SDoC process would be prohibited; as we discussed above, under our current rules, responsible parties always have the option of seeking equipment authorization through the Commission's equipment certification procedures. Under our proposed rules, responsible parties would be required to use the certification procedures for any "covered" equipment, as such equipment will no longer have the option of obtaining equipment authorization through the SDoC processes. This proposal will help ensure consistent application of our proposed prohibition on further equipment authorization of any "covered" equipment by requiring use of only one process, which includes the Commission's more active oversight and proactive guidance when working directly with TCBs prior to any equipment authorization in the first place, and in guiding appropriate post-market surveillance after any equipment authorization. We find this approach consistent with the public interest.

59. We seek comment on the specific information that must be included in the SDoC compliance statement that will ensure that responsible parties do not use the SDoC process for "covered" equipment. This compliance statement would need to be sufficiently complete to require a responsible party to exercise necessary diligence with respect to the equipment that it is subjecting to the SDoC process that will ensure that it is attesting, in clear terms, that the equipment (or any component part thereof) is not produced or provided by any entity that has produced or provided "covered" equipment on the Covered List. This compliance statement should be crafted in such as manner as to assist responsible parties in identifying equipment that can no longer be processed through the SDoC process while also ensuring that responsible parties are held accountable, by their compliance statement, for any misrepresentations or violation of the prohibition that we are proposing.

60. What steps should the Commission take to help inform responsible parties that use the SDoC process of this proposed prohibition , as well as the requirement that any "covered" equipment (including component parts) must be subject to the equipment certification process? We note that our rules allow many entities to take on the role of a responsible party under our part 2 rules, including retailers and parties performing modifications to equipment. We seek comment on how best to ensure that all responsible parties that use the SDoC processes to enable importing or marketing equipment in the United States understand and comply with our proposed revisions with respect to "covered" equipment on the Covered List.

61. As noted above, the Commission can specifically request that the responsible parties provide information on any equipment to the Commission that it has processed through the SDoC process.[178] Under our proposal, in an effort to ensure that responsible parties are complying with our

---

or individual performing the testing; description of the equipment; and/or the "compliance information" required under the rules). *See* 47 CFR § 2.1077 (Compliance information). The Commission's rules include procedures wherein the Commission can suspend action on application or require forfeiture. *See* 47 CFR §§ 2.945(b)(5), 2.945(c). Upon request by the Commission, each responsible party must make its manufacturing plant and facilities available for inspection. 47 CFR § 2.945(d).

[178] 47 CFR §§ 2.906(a); 2.945(b)(1) (Commission may request that the responsible party or any other party marketing the equipment submit a sample); 2.945(c) (upon request by the Commission, each responsible party shall submit copies of records required under the Commission's rules, including – the original design drawings and specification; procedures for inspection and testing; test results; actual date of testing; name of the test lab, company, or individual performing the testing; description of the equipment; and/or the "compliance information" required under the rules). *See* 47 CFR § 2.1077 (Compliance information). The Commission's rules include procedures wherein the Commission can suspend action on application or require forfeiture. *See*47 CFR §§ 2.945(b)(5),

(continued….)

prohibition, the Commission would exercise its equipment authorization oversight, as appropriate, in requesting that the responsible parties provide information – e.g., an equipment sample , representative data demonstrating compliance, and the compliance statement itself – regarding particular equipment to the Commission. We seek comment on what kinds of situations in which such requests might be appropriate. What kinds of information might inform the Commission's consideration as to whether any equipment may have been inappropriately processed through the SDoC process, thus triggering the Commission's request for information from the responsible party to make sure that no violation of the Commission's prohibition have occurred?

62. As we have discussed, PSHSB will periodically publish updates to identify the "covered" equipment on the Covered List.[179] As with the equipment certification proposals above, we would direct that OET expeditiously to take all the appropriate steps (e.g., updating as necessary the information that SDoC applicants must make to establish that no newly identified "covered" equipment is associated with the application to reflect those updates), consistent with the rules and procedures that the Commission ultimately adopts regarding the SDoC rules in this proceeding. We invite comment on appropriate means for OET to include updates of the "covered" equipment in an expeditious fashion in ways that best ensure that applicants, responsible parties, and other interested parties will comply with the proposed prohibitions that we have proposed.

63. Finally, we seek comment on whether there are other rule revisions or clarifications to the SDoC rules and processes that the Commission should make consistent with our goals to prohibit authorization of "covered" equipment. Commenters should explain their suggestions in sufficient detail, including the reasoning behind the suggestions and associated issues (e.g., implementation).

(iv) Legal authority

64. Adopting rules that take security into consideration in the equipment authorization process would serve the public interest by addressing significant national security risks that have been identified by this Commission in other proceedings, and by Congress and other federal agencies, and doing so would be consistent with the Commission's statutory "purpose of regulating interstate and foreign commerce in communication by wire and radio … for the purpose of the national defense [and] for the purpose of promoting safety of life and property through the use of wire and radio communications."[180] We tentatively conclude that doing so is not specifically authorized by the Secure Networks Act itself, pursuant to which the Commission adopted the Covered List. However, the Commission has broad authority to adopt rules, not inconsistent with the Communications Act, "as may be necessary in the execution of its functions."[181] We believe that, in order to ensure that the Commission's rules under the Secure Networks Act effectively preclude use of equipment on the Covered List by USF recipients as contemplated by Congress, it is necessary to rely on the Commission's established equipment authorization procedures to restrict further equipment authorization, and the importation and marketing, of such devices in the first instance. As discussed above,[182] the Commission also relies on the equipment authorization process to implement other statutory duties, including the duty to promote efficient use of the radio spectrum,[183] our duties under the National Environmental Policy Act

2.945(c). Upon request by the Commission, each responsible party must make its manufacturing plant and facilities available for inspection. 47 CFR § 2.945(d).

[179] *Covered List Public Notice* at 2.

[180] 47 U.S.C. § 151.

[181] 47 U.S.C. § 154(i).

[182] *See supra* para. [[[20]]]

[183] 47 CFR § 2.901; *see* 47 U.S.C. § 303(g) (requiring the Commission to "generally encourage the larger and more effective use of radio in the public interest").

to regulate human RF exposure,[184] our duty to ensure that mobile handsets are compatible with hearing aids,[185] and our duty to deny federal benefits to certain individuals who have been convicted multiple times of federal offenses related to trafficking in or possession of controlled substances.[186] We believe that these processes can and should also serve the purpose of fulfilling other Commission responsibilities under the Secure Networks Act, and we seek comment on that issue.

65. We also believe that other authorities in the Communications Act of 1934, as amended, provide authority for the Commission to rely on for the proposed modifications to its rules and procedures governing equipment authorization. Since Congress added section 302 to the Act, the Commission's part 2 equipment authorization rules and processes have served to ensure that RF equipment marketed, sold, imported, and used in the United States complies with the applicable rules governing use of such equipment.[187] That section authorizes the Commission to, "consistent with the public interest, convenience, and necessity, make reasonable regulations … governing the interference potential of devices which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications."[188] Regulations that we adopt in implementing that authority "shall be applicable to the manufacture, import, sale, offer for sale, or shipment of such devices and … to the use of such devices."[189] The authorization processes are primarily for the purpose of evaluating equipment's compliance with technical specifications intended to minimize the interference potential of devices that emit RF energy. As noted above, however, these rules are also designed to implement other statutory responsibilities. We seek comment on the scope of our authority to rely on such rules to effectuate other public interest responsibilities, including our section 303(e) authority to "[r]egulate the kind of apparatus to be used with respect to its external effects."[190] Does Congress's inclusion of the phrase "to be used," rather than "used," give the Commission authority to prevent the marketing and sale of equipment in addition to preventing licensees and others from using such equipment?

66. Alternatively, does the "public interest" phrase in section 302 itself provide independent authority to deny equipment authorization to equipment deemed to pose an unacceptable security risk? Section 302(a) directs the Commission to make reasonable regulations consistent with the public interest governing the interference potential of devices; it would appear to be in the public interest not to approve devices capable of emitting RF energy in sufficient degree to cause harmful interference to radio communications if such equipment has been deemed, pursuant to law, to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons. We seek comment on this tentative conclusion.

67. We note and seek comment on a potential alternative basis for such security rules. The Communications Assistance for Law Enforcement Act (CALEA)[191] includes security requirements that

[184] 47 CFR §§ 2.1091-.1093.

[185] 47 CFR §§ 2.925(b)(2), 2.1033(d); *see* 47 U.S.C. § 610.

[186] 47 CFR § 1.2002(a); *see* 21 U.S.C. § 862 (Anti-Drug Abuse Act of 1988).

[187] *See Equipment Authorization of RF Devices*, Docket No. 19356, Report and Order, 39 Fed. Reg. 5912, 5912, para. 2 (1970).

[188] 47 U.S.C. § 302(a)(1).

[189] 47 U.S.C. § 302(a)(2).

[190] 47 U.S.C. § 303(e).

[191] 47 U.S.C. §§ 1001-1010.

apply directly to equipment intended for use by providers of telecommunications services.[192] Section 105 requires telecommunications carriers to ensure that the surveillance capabilities built into their networks "can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission,"[193] and the Commission has concluded that its rule prohibiting the use of equipment produced or provided by any company posing a national security threat implements that provision.[194] The Commission is required to prescribe rules necessary to implement CALEA's requirements.[195] Would rules prohibiting authorization of equipment on the Covered List, or that otherwise poses security risks, be justified as implementation of CALEA?

68. As noted above, we believe the Commission has ancillary authority under section 4(i) of the Act to adopt these revisions to its part 2 rules as reasonably necessary to the effective enforcement of the Secure Networks Act. We also tentatively conclude that such rules would be consistent with our specific statutorily mandated responsibilities under the Communications Act to make reasonable regulations consistent with the public interest governing the interference potential of electronic devices, to protect consumers through our oversight of common carriers under Title II of that Act, and to prescribe the nature of services to be rendered by radio licensees under section 303(b) of that Act. We seek comment on this reasoning as well. We also seek comment on any other sources of authority for our proposed rules.

(v) Cost-effectiveness analysis

69. Our proposed revisions to the Commission's equipment authorization rules and processes to prohibit authorization of any "covered" equipment on the Covered List would apply only to equipment that has been determined by other agencies to pose "an unacceptable risk" to national security. The Commission has already concluded that it has no discretion to disregard determinations from these sources, which are enumerated in section 1.50002(b) of its rules. Hence, we accept the determination of these expert agencies.

70. Because we have no discretion to ignore these determinations, we believe that a conventional cost-benefit analysis – which would seek to determine whether the costs of our proposed actions exceed their benefits – is not directly called for. Instead, we will consider whether the proposed actions would be a cost-effective means to prevent this dangerous equipment from being introduced into our nation's communications networks.

71. We therefore seek comment on the cost-effectiveness of our proposed revisions to the rules and procedures associated with the Commission's equipment authorization rules under part 2. Do our proposed rules promote our goals of ensuring that our national security interests are adequately protected from equipment on the Covered List, while simultaneously continuing our mission of making communications services available to all Americans? Are there alternative approaches that would achieve this goal in a more cost-effective manner?

b. Devices Exempt from the Requirement of an Equipment

[192] For this purpose, *telecommunications service* includes facilities-based broadband Internet access services and interconnected VoIP services, notwithstanding the classification of those services under the Communications Act. *See Communications Assistance for Law Enforcement Act and Broadband Access and Services*, ET Docket No. 04-295, First Report and Order and Further Notice of Proposed Rulemaking, 20 FCC Rcd 14989 (2005), *pet. for rev. denied, American Council on Educ. v. FCC*, 451 F.3d 226 (D.C. Cir. 2006).

[193] 47 U.S.C. § 1004.

[194] *Supply Chain First Report and Order*, 34 FCC Rcd at 11436-37, paras. 35-36.

[195] 47 U.S.C. § 229.

Authorization

72. *Background.* Under the Commission's rules, certain types of unlicensed RF devices are exempt from demonstrating compliance under one of the equipment authorization procedures (either certification or SDoC).[196] In general, exempt part 15 devices generate such low levels of RF emission that they have virtually no potential for interfering with the authorized radio services.[197] In other services, the Commission has determined that because operators must be individually licensed and responsible for their stations (e.g., Amateur Radio Service) or the type of operation poses low risk of harmful interference, such an exemption is warranted.[198] Exempt devices still are required to comply with general conditions of operation.[199] In other words, if an exempt device causes interference to other radio services, then the operator of that device must cease operating the device upon notification from the FCC and must remedy the interference.

73. The most diverse set of exempted devices operate under our part 15 unlicensed device rules. The categories of part 15 exempt devices include incidental radiators,[200] unintentional radiators exempt under section 15.103, and subassemblies exempt under section 15.101. Specifically, section 15.103 of the Commission's rules provides that certain unintentional radiators, which are subject to the general conditions of operation provided in part 15,[201] are exempt from the specific technical standards and other requirements of part 15. This includes: (1) digital devices used exclusively in any transportation vehicle as an electronic control or power system equipment used by a public utility or in an industrial plant, as industrial, commercial, or medical test equipment, or in an appliance (e.g., microwave oven, dishwasher, clothes dryer, air conditioner, etc.); (2) specialized medical digital devices; (3) digital devices that have very low power consumption (i.e., not exceeding 6 nW); (4) joystick controllers or similar devices used with digital devices; and (5) digital devices that both use and generate a very low frequency (i.e. less than 1.705 MHz) and which do not operate from the AC power lines or contain provisions for operation while connected to the AC power lines.[202] Digital device subassemblies also are exempt from equipment authorization under section 15.101. Examples of subassemblies include circuit boards, integrated circuit chops, and other components that are completely internal to a product that do not constitute a final product. These include internal memory expansion boards, internal disk drives, internal disk drive controller boards, CPU boards, and power supplies. Subassemblies may be sold to the general public or to manufacturers for incorporation into a final product.

74. *Discussion.* We recognize that "covered" equipment potentially could include equipment that currently is exempt from the need to demonstrate compliance under the Commission's equipment authorization processes, which, to date, has looked only at the RF emissions capability of equipment. As

---

[196] For example, devices described in section 15.103 are not subject to any equipment authorization procedures. Similarly, section 90.203 generally requires all devices that operate under that part to be certified but contains provisions that exempts certain devices from that requirement. Under Part 25, only portable earth station transceivers are subject to equipment certification procedures; all other Part 25 equipment is exempt for equipment authorization procedures. *See* 47 CFR § 25.129. Also, under Part 97 only external power amplifiers used in the Amateur Radio Service are required to obtain equipment certification; all other equipment is exempt from equipment authorization procedures. *See* 47 CFR § 97.315.

[197] *Revision of Part 15 of the Rules Regarding the Operation of Radio Frequency Devices without an Individual License*, GN Docket No. 87-389, Notice of Proposed Rulemaking, 2 FCC Rcd 6135, 6140, para. 39 (1987).

[198] *See, e.g.*, 47 CFR § 97.315.

[199] *See* 47 CFR § 15.5.

[200] An incidental radiator is a device that generates RF energy during the course of its operation although the device is not intentionally designed to generate or emit RF energy. 47 CFR § 15.3(n).

[201] *See* 47 CFR §§ 15.5, 15.29.

[202] 47 CFR § 15.103.

noted above, most devices that are generally exempt from the Commission's equipment authorization requirements typically have such low RF emissions that they present virtually no potential for causing harmful interference to with the authorized radio services. However, our concerns in relation to security considerations that pose unacceptable risks to our nation's communications networks are distinct from our concerns related to interference to authorized services. As such, we find it necessary to assess our regulation of otherwise exempt devices in relation to security concerns.

75. Accordingly, we seek comment on whether the Commission should consider possible revisions or clarifications to the Commission's rules to address issues related to "covered" equipment and the potential of such equipment, regardless of RF emissions characteristics, to pose an unacceptable risk to U.S. networks or users. We seek comment on whether the Commission should revise its rules to no longer provide an equipment authorization exemption to "covered" equipment. We seek comment on whether such a provision, if adopted, should apply only to part 15 unlicensed devices or should include any device, regardless of rule part under which it operates, in our consideration of possible revisions or clarifications to the Commission's rules to address issues related to "covered" equipment and the potential of such equipment, regardless of RF emissions characteristics, to nonetheless pose an unacceptable risk to U.S. networks or users. We also ask whether we should require that any equipment (in whole or in part), regardless of claim of exemption, that is produced or provided by any entity that has produced or provided "covered" equipment on the Covered List, to be processed pursuant to the Commission's certification rules and processes (similar to our proposal requiring use of the certification process for such equipment instead of continued use of the SDoC process).

76. Currently, devices that are exempt from the equipment authorization requirement are not subject to FCC testing, filing, or record retention requirements. Such devices ordinarily would come to the attention of the Commission only in the event that harmful interference with other devices becomes an issue. In order to determine whether otherwise exempt "covered" equipment may present a security concern, the Commission would need to implement some means by which to identify such equipment that is in use in the United States. We seek comment on possible methods that the Commission could implement to identify otherwise exempt equipment. We could, for instance, implement a registration system for otherwise exempt equipment. Such a system could require responsible parties to notify the Commission of the marketing, importation, or operation of otherwise exempt equipment, to include identification of the responsible party, manufacturer, or importer and the general operating parameters of the equipment. Another example includes an attestation at time of marketing or import that the equipment is not "covered." What are some potential burdens to responsible parties or other entities that would arise in connection with such a registration or attestation system? In what ways and to what extent would such burdens be acceptable to responsible parties to help protect the U.S. against the related security concerns? What type of information, and from which entities, should the Commission collect in order to identify otherwise exempt "covered" equipment? How many responsible parties would be impacted by these potential information collections and in what way would it impact their ability to conduct business?

77. We discussed above the legal authority associated with the Commission's proposal to prohibit authorization of "covered" equipment in its equipment authorization process. We tentatively conclude legal bases enunciated above also provide, pursuant to Section 302 and Section 4(i) of the Act, provide for actions that the Commission might take with respect to precluding "covered" equipment from being exempted from the equipment authorization process. We seek comment on this tentative conclusion.

78. If we were to conclude that our rules should be revised to prohibit certain "covered" equipment from being exempted from the equipment authorization processes, this action would apply only to equipment that has been determined by other agencies to pose "an unacceptable risk" to national security. Because we have no discretion to ignore these determinations, we believe that a conventional cost-benefit analysis – which would seek to determine whether the costs of our proposed actions exceed their benefits – is not necessary. Instead, as we have discussed above, we will consider whether the

proposed actions would be an effective means to prevent this dangerous equipment from being introduced into our nation's communications networks.

c. Revoking Equipment Authorizations

79. The actions that we propose above would serve to prohibit any prospective authorization of "covered" communications equipment on the Covered List as posing an unacceptable risk to national security. Those proposed actions do not, however, address whether the Commission could or should revoke any existing equipment authorizations of such "covered" communications equipment, and if so, the processes for doing so. We address those issues here.

80. *Background*. Section 2.939 sets forth the Commission's rules for revoking authorizations of equipment.[203] Section 2.939(a)(1) provides that the Commission may revoke an equipment authorization "[f]or false statements or representations either in the application or in materials or response submitted in connection therewith" or in records that the responsible party is required to maintain about the authorized equipment (e.g., drawings and specifications, description of the equipment, any test report, equipment compliance information).[204] Section 2.939(a)(2) states that the Commission may revoke an equipment authorization "[i]f upon subsequent inspection or operation it is determined that the equipment does not conform to the pertinent technical requirements or to the representations made in the original application."[205] Section 2.939(a)(3) provides that the Commission may revoke an equipment authorization "[i]f it is determined that changes have been made in the equipment other than those authorized by the rules or otherwise expressly authorized by the Commission."[206] Section 2.939(a)(4) provides that the Commission may revoke any equipment authorization "[b]ecause of conditions coming to the attention of the Commission which would warrant it in refusing to grant an original application."[207] As set forth in section 2.939(b), the procedures for revoking an equipment authorization are the same procedures as revoking a radio station license under Section 312 of the Communications Act.[208] Finally, under section 2.939(c), the Commission also "may withdraw any equipment authorization in the event of changes in its technical standards."[209]

81. *Discussion.* If we adopt the rules proposed above to prohibit any further authorization of "covered" equipment on the Covered List, we seek comment here on the extent to which the Commission should revoke any existing equipment authorizations of such "covered" equipment pursuant to our section 2.939 revocation rules. We note that if the Commission revoked an existing equipment authorization, the marketing of that equipment would be prohibited pursuant to part 2 Subpart I, per section 2.803(b),[210] and import and marketing would be prohibited pursuant to part 2 Subpart K, per sections 2.1201(a) and 2.1204(a).[211]

---

[203] 47 CFR § 2.939.

[204] 47 CFR § 2.939(a)(1). The "responsible party" is required to maintain records relating to authorized equipment pursuant to section 2.938 of the Commission's equipment authorization rules, 47 CFR § 2.938, and which includes compliance information as specified in section 2.1077 of the Commission's rules, 47 CFR § 2.1077.

[205] 47 CFR § 2.939(a)(2).

[206] 47 CFR § 2.939(a)(3).

[207] 47 CFR § 2.939(a)(4).

[208] *See* 47 CFR § 2.939(b); 47 U.S.C. § 312.

[209] 47 CFR § 2.939(c). The procedure to be followed will be set forth in the order promulgating such new technical standards (after appropriate rulemaking proceedings) and will provide a suitable amortization period for equipment in hands of users and in the manufacturing process. *Id.*

[210] 47 CFR § 2.803(b).

[211] 47 CFR §§ 2.1201(a), 2.1204(a).

82. We tentatively conclude that Sections 2.939(a)(1) and (2) would apply to "covered" equipment,[212] such that the Commission has authority to revoke any existing equipment authorizations that may have been granted under false statements or representations (including non-disclosure) concerning whether, an equipment authorization application that was subsequently granted had in fact included "covered" equipment (in whole or as a component part).[213] This would enable the Commission to revoke any equipment authorizations that are granted after adoption of the rules proposed in this Notice, even if the TCBs or the Commission had not acted to set aside the grant within the 30-day period following the posting of the grant on the Equipment Authorization System (EAS) database. We seek comment on this tentative conclusion.

83. To assure that otherwise authorized equipment is not subsequently replaced by any "covered" equipment (whether in whole or with component part(s) of "covered" equipment), we also tentatively conclude that section 2.939(a)(3) would apply, and that the Commission can revoke an existing equipment authorization if changes have been made in the equipment other than those authorized by the rules or otherwise expressly authorized by the Commission.[214] We seek comment on these and any other scenarios that implicate our need to revoke an existing equipment authorization to exclude "covered" equipment from the U.S. market.

84. We also seek comment on other circumstances that would merit Commission action to revoke any existing authorization of "covered" equipment. Under what circumstances should the Commission revoke an existing authorization? For instance, to what extent does section 2.939(a)(4), which allows revocation "[b]ecause of conditions coming to the attention of the Commission which would warrant it in refusing to grant an original application,"[215] provide guidance? Specifically, if the Commission would not have granted an application with equipment from an entity on the Covered List under newly adopted rules, then could the Commission use section 2.939(a)(4) to revoke an equipment authorization with said equipment that had been granted prior to the adoption of the rule?[216] We seek comment on this approach and on any other approach or particular circumstances that would merit Commission action to revoke any existing authorization that concerns "covered" equipment on the Covered List.

85. We seek comment the applicability of section 2.939(c), which states that the Commission also "may withdraw any equipment authorization in the event of changes in its technical standards,"[217] with regard to revocation of authorizations that include "covered" equipment. In the event the Commission were, as we propose here, to adopt rules barring new equipment authorizations for equipment on the Covered List, we tentatively conclude that such a change should constitute a change to the Commission's technical standards that could warrant withdrawal of equipment authorizations that are

[212] 47 CFR § 2.939(a)(1)-(2).

[213] *Shenzhen Tangreat Technology Co., Ltd.*, 30 FCC Rcd 3501,3505, paras. 12-14 (EB 2015) (*Shenzhen*) ("substantial and material questions exist as to whether the authorization should be revoked because the information in the application was false or misleading").

[214] *Shenzhen*, 30 FCC Rcd at 3505-06, paras. 15-17 (Commission investigation demonstrated that the equipment marketed does not match the specifications described in the granted application).

[215] 47 CFR § 2.939(a)(4).

[216] *Shenzhen*, 30 FCC Rcd at 3506, paras. 18-20 (when Commission investigation determined device was a radio frequency jammer, "substantial and material questions exist as to whether the application should have been granted"), *see also J Communications Co., Ltd.*, 19 FCC Rcd 10643, 10645, para. 9 (EB 2004) (revoking GMRS radios because the Commission could have denied the original equipment authorization application for the devices "had this fact been made known to the Commission").

[217] 47 CFR § 2.939(c). The procedure to be followed will be set forth in the order promulgating such new technical standards (after appropriate rulemaking proceedings) and will provide a suitable amortization period for equipment in hands of users and in the manufacturing process. *Id.*

contrary to these new rules. We seek comment.

86. In addition, we seek comment on the specific procedures the Commission should use if and when it seeks to revoke an existing equipment authorization. Section 2.939(b) requires that revocation of an equipment authorization must be made in the "same manner as revocation of radio station licenses,"[218] and thus presumably would include the requirement that the Commission serve the grantee/responsible party with an order to show cause why revocation should not be issued and must provide that party with an opportunity for a hearing.[219] We seek comment on this requirement. What precisely are the procedures that the Commission should employ if seeking to revoke particular "covered" equipment? As we discussed above, section 2.939(c) authorizes the Commission to withdraw any equipment authorization in the event of changes in its technical standards."[220] Pursuant to this provision, should we provide a suitable amortization period for equipment already in the hands of users or in the manufacturing process? If so, what would that be? What other factors should we consider that might warrant revocation under our new rules, such as those applicable to Title III licenses under section 312 of the Communications Act?[221] Should we revise or clarify the existing requirements to enable the Commission to revoke authorizations of this "covered" equipment given that it already has been determined that the equipment poses an unacceptable risk?

87. In considering whether any existing equipment authorizations of "covered" equipment should be revoked, is there some process in which the Commission should engage to help identify particular equipment authorizations that should be considered for revocation? What process should we use to identify equipment authorizations for revocation? For example, to what extent might we rely on others' reports of a violation, and to what extent might such reports need to be supported in our record or independently verified? If we were to conclude that revocation may be appropriate regarding particular "covered" equipment, this action would apply only to equipment that has been determined by other agencies to pose "an unacceptable risk" to national security. We nonetheless recognize the need to avoid taking actions that are overbroad in terms of affecting users of the equipment or would require removal of this equipment faster than it reasonably can be replaced. If we conclude that revocation may be appropriate regarding particular "covered" equipment, we seek comment on the appropriate and reasonable transition period for removing that particular equipment. This could include a transition period for non-conforming equipment to make any necessary modifications to communications equipment or services in order to remove the "covered equipment" (in whole or as a component) from that equipment or service? To what extent should we apply different transition periods to different equipment authorizations that we revoke? Are there any situations that might merit immediate compliance with the new equipment restrictions?

88. Finally, we seek comment on whether the Commission should make any revisions to section 2.939. Should this section be revised and/or clarified to specifically include "covered" equipment or whether the rule should be clarified to better encompass our intent in this rulemaking? What specific revisions might be appropriate for consideration?

2. Competitive Bidding Certification

89. *Background.* The Commission's competitive bidding process requires each applicant to make various certifications as a prerequisite for participation in an auction.[222] Requiring certifications as

[218] 47 CFR § 2.939(b).

[219] *See* 47 U.S.C. § 312(c).

[220] 47 CFR § 2.939(c).

[221] 47 U.S.C. § 312.

[222] *See* Section II.C., above.

a condition of participation guards against potential harms to the public interest before the harms could occur.[223]

90. As described above, the Commission has designated Huawei and ZTE, and their subsidiaries, parents, or affiliates, as companies that pose a national security threat to the integrity of communications networks and the communications supply chain.[224] As a result of this determination, funds from the Commission's Universal Service Fund may no longer be used to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by these covered companies.

91. In reaching this determination, the Commission noted Huawei's and ZTE's ties to the Chinese government and military apparatus, along with Chinese laws obligating it to cooperate with requests by the Chinese government to use or access its systems.[225] However, it also is well-established that the Chinese government helps fuel Huawei's growth by deploying powerful industrial policies to make Huawei equipment cheaper to deploy than the alternatives.[226] These policies include both direct subsidies to Huawei and state-funded export financing.

92. To illustrate, a recent report by the Center for American Progress found that China's state-owned banks have provided billions of dollars to Huawei's customers.[227] According to the report, these loans "can make Huawei impossible to beat—even if competitors can match the company's state-subsidized prices—because China's state banks offer packages that commercial banks generally cannot match."[228] These loans may be run through Huawei or provided directly to Huawei's customers.

93. We note that the nature of state support for Huawei and ZTE has shifted over time. Recently, the Commission has observed how state-funded export financing may provide substantial funding to mobile operators already using equipment from Huawei or ZTE prior to national spectrum auctions in other countries. In one recent case, a Huawei customer was able to substantially outbid a rival new entrant in a spectrum auction—thereby denying entry to a new competitor that was planning on using trustworthy equipment in its 5G build-out.

94. Distortionary financing intended to support participation in spectrum auctions of network operators who then deploy covered equipment and services may raise concerns about risks to the national security of the United States and the security and safety of United States persons. We consider here the benefits of protecting against such risks prior to the start of a Commission auction.

95. *Discussion.* Given recent developments internationally, we seek comment on whether the Commission should require an applicant to participate in competitive bidding to certify that its bids do not and will not rely on financial support from any entity that the Commission has designated under Section 54.9 of its rules as a national security threat to the integrity of communications networks or the communications supply chain. Could such support implicate the kinds of influence over the applicant that would pose risks to national security? Or could it distort auction outcomes in ways that would pose risks to national security? What challenges would an applicant have in satisfying such a certification, given potential uncertainties regarding the ultimate origin of financial support? Can the certification be

[223] This timing also furthers the public interest in rapid deployment of new technologies, products, and services by protecting against subsequent license application denials and repetitive assignments of the same licenses.

[224] *See generally Huawei Designation Order*, 35 FCC Rcd 6604, *ZTE Designation Order*, 35 FCC Rcd 6633,

[225] *Huawei Designation Order*, 35 FCC Rcd at 6609, paras. 13-14.

[226] Chuin-Wei Yap, *State Support Helped Fuel Huawei's Global Rise*, Wall Street Journal (Dec. 25, 2019), https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736

[227] Melanie Hart and Jordan Link, Center for American Progress, *There Is a Solution to the Huawei Challenge* (Oct. 14, 2020), https://www.americanprogress.org/issues/security/reports/2020/10/14/491476/solution-huawei-challenge/

[228] *Id.* at para. 25.

crafted to address these challenges? Do these uncertainties present difficulties for the Commission in enforcing the certification? How can these difficulties be mitigated?

96. If we adopt a requirement that an applicant certify that its bids do not and will not rely on financial support by an entity designated by the Commission as a national security threat, should the certification be limited to just the entities so designated by the Commission under Section 54.9 or be more expansive? What are the challenges with including indirect provision of financing in the certification and how can they be mitigated to ensure it accomplishes its purpose? Should the certification be expanded to include an identified set of related entities, e.g., entities subject to control by an entity designated by the Commission? What entities should such a set include? How does the fungibility of financial resources complicate compliance? How can enforcement challenges be alleviated?

B. Notice of Inquiry

97. The above Notice of Proposed Rulemaking proposes direct action to limit the presence of untrusted equipment and services in U.S. networks. We recognize, however, that ensuring continued U.S. leadership requires that we also explore opportunities to spur trustworthy innovation for more secure equipment. In this Notice of Inquiry, we seek comment on how the Commission can leverage its equipment authorization program to encourage manufacturers who are building devices that will connect to U.S. networks to consider cybersecurity standards and guidelines.

98. The development and implementation of effective cybersecurity practices requires the continued cooperation and participation of all stakeholders. In this regard, we observe that both the public and private sectors have come together to develop measures to protect the integrity of communications networks and guard against malicious or foreign intrusions that can compromise network services, steal proprietary information, and harm consumers. In particular, the National Institute of Standards and Technology (NIST) has worked with both industry and government to produce multiple cybersecurity frameworks and other forms of guidance that help protect the integrity of communications networks. Pursuant to Executive Order No. 13636, NIST began working with public and private stakeholders to develop a voluntary cybersecurity framework designed to reduce risks to critical infrastructure.[229] This framework consists of "voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk."[230] Originally issued in 2013, the NIST cybersecurity framework was updated in 2018 to clarify and refine certain aspects and better explain how entities should use the framework to improve their cybersecurity practices.[231] In addition, among other organizations, the Federal Trade Commission (FTC) has been active in cybersecurity matters for years, bringing multiple enforcement actions against firms for having poor cybersecurity practices[232] and offering cybersecurity guidance for Internet of Things (IoT) devices as

[229] Exec. Order No. 13636, 78 Fed. Reg. 11737 (Feb. 19, 2013; *see* Nat'l Inst. of Standards & Tech., *Cybersecurity Framework: New to Framework* (last updated Sept. 23, 2020), https://www.nist.gov/cyberframework/new-framework.

[230] *See* Nat'l Inst. of Standards & Tech., *Cybersecurity Framework: New to Framework* (last updated Sept. 23, 2020), https://www.nist.gov/cyberframework/new-framework.

[231] *See* Nat'l Inst. of Standards & Tech., *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1* (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[232] *See, e.g.*, Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236 (2015) (affirming a complaint brought against Wyndham Worldwide Corp. for poor cybersecurity practices on the hotel chain's information systems that resulted in the theft of hundreds of thousands of consumers' personal and financial data); Press Release, *FTC Gives Final Approval to Lenovo Settlement*, Fed. Trade Comm'n (Jan. 2, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/ftc-gives-final-approval-lenovo-settlement (approving a settlement stemming from a complaint about pre-loaded software on laptops that compromised security protections in order to deliver ads to consumers).

early as 2015.[233] Further, industry trade groups, including CTIA–The Wireless Association,[234] GSMA,[235] the ioXt Alliance,[236] and TIA[237] have produced cybersecurity guidance applicable to various sectors of the communications industry. Non-profit standards bodies and think tanks have also produced cybersecurity guidance that could be useful to the communications industry.[238]

99. More recently, NIST has developed a Cybersecurity for the Internet of Things (IoT) program, which specifically "supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed."[239] Devices that operate as part of the Internet of Things (IoT) specifically raise concerns about security risks. For example, NTIA has recognized that connected devices in the IoT can extend the scope and scale of automated, distributed attacks.[240]

100. This Cybersecurity for IoT program has produced multiple reports, but perhaps most notable is Internal Report 8259, released in May 2020.[241] This *NIST IoT Report* details activities that "can help manufacturers lessen the cybersecurity-related efforts needed by customers, which in turn can reduce the prevalence and severity of IoT device compromises and the attacks performed using compromised devices."[242] The NIST IoT Report is voluntary guidance intended to help promote the best available practices for mitigating risks to IoT security. The report describes six recommended foundational cybersecurity activities that manufacturers should consider performing to improve the securability of the new IoT devices they make. They include identifying expected customers and users and defining expected use cases; researching customer cybersecurity needs and goals; determining how to address customer needs and goals; planning for adequate support of customer needs and goals; defining approaches for communicating to customers; and deciding what to communicate to customers and how to communicate it. These activities are intended to fit within a manufacturer's existing development

[233] Fed. Trade Comm'n, *Careful Connections: Building Security in the Internet of Things* (Jan. 2015), https://www.bulkorder.ftc.gov/system/files/publications/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf.

[234] CTIA–The Wireless Assoc., *IoT Cybersecurity Certification Program Management Document: Version 1.1* (May 2019), https://api.ctia.org/wp-content/uploads/2019/05/ctia_IoT_cybersecurity_pmd_ver-1_1.pdf.

[235] Jenny Lu, *Maintaining a Robust Device Identity System: Introducing the GSMA TAC and IMEI Integrity Framework*, GSMA (Sept. 11, 2019), https://www.gsma.com/services/2019/09/11/tac-and-imei-integrity-framework/.

[236] ioXt All., *ioXt Certification Program* (last visited May 21, 2021), https://www.ioxtalliance.org/get-ioxt-certified.

[237] Telecomm. Indus. Ass'n, *SCS 9001: The First ICT-Specific Standard for Global Supply Chain Security* (last visited May 21, 2021), https://tiaonline.org/what-we-do/technology-programs/supply-chain-security/scs-9001-ict-specific-standard-for-global-supply-chain-security/ (noting that Version 1.0 of the standard will be released in Q3 2021).

[238] *See, e.g.*, Internet Soc'y, *Internet of Things (IoT) Trust Framework v2.5* (May 22, 2019), https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/.

[239] Nat'l Inst. of Standards & Tech., *NIST Cybersecurity for IoT Program* (last updated Mar. 19, 2021), https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program.

[240] *https://www.ntia.doc.gov/files/ntia/blogimages/botnet_road_map_status_update.pdf*

[241] Nat'l Inst. of Standards & Tech., *Foundational Cybersecurity Activities for IoT Device Manufacturers*, Internal Report 8259 (May 2020) (*NIST IoT Report*), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf.

[242] *Id.* In the *NIST IoT Report*, six activities are suggested to help manufacturers produce IoT devices with better cybersecurity, four of which primarily impact the pre-market phase — before the IoT devices have been sold — while the other two primarily impact the post-market phase — after the devices have been sold. Substantial guidance and examples are provided for each of these suggested activities. *Id.* at 6-23.

process.

101. We seek comment on how the Commission can leverage its equipment authorization program to help address the particular security risks that are associated with IoT devices. Should the Commission encourage manufacturers of IoT devices to follow the guidance in the *NIST IoT Report*? If the Commission were to utilize the equipment authorization process to incentivize better cybersecurity practices, either for all devices or specifically for IoT devices, what form should such provisions take and how would such a program be structured most effectively? Should the FCC allow IoT manufacturers to voluntarily certify during the equipment authorization process that they have performed or plan to perform the activities described in the guidance? Which standards should be considered? Are there other incentives or considerations that could encourage manufacturers to build security into their products? Commenters should discuss the potential costs and benefits associated with their proposals or with the potential approaches discussed herein.

102. We observe that the Consumer Technology Association (CTA) published a white paper offering guidance for how government, industry, and consumers can all work together to promote better cybersecurity practices going forward.[243] In this white paper, CTA encourages public-private partnerships to develop and deploy risk-based approaches to cybersecurity,[244] and argues that "neither the new Administration nor Congress should embrace rules, product labels or certification regimes for consumer IoT."[245] They claim that "[c]ybersecurity mandates, pre-market 'approval,' and government certification or labeling of IoT devices are likely to require an enormous bureaucracy and have unintended consequences."[246] We seek comment on these views. Are there any gaps in the *NIST IoT Report* or other federal efforts to address IoT security that the Commission could help address?

103. We recognize that consideration of how to incentivize cybersecurity best practices through our equipment authorization process aligns closely with the recently issued Executive Order 14028, which directs NIST to work with the Federal Trade Commission and other agencies to develop a labeling program to identify specific IoT cybersecurity criteria and provide that information to consumers.[247] While the Director of NIST has not yet identified the agencies that will participate in the forthcoming IoT cybersecurity labeling program, we seek comment on whether the Commission can support these efforts, either directly or indirectly. If so, how?

IV. PROCEDURAL MATTERS

104. *Initial Regulatory Flexibility Analysis.* As required by the Regulatory Flexibility Act of 1980 (RFA),[248] as amended (RFA), the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities of the proposals addressed in this Notice of Proposed Rulemaking and Notice of Inquiry. The IRFA is found in Appendix B. Written public comments are requested on the IRFA. These comments must be filed in accordance with the same filing deadlines for comments on the Notice of Proposed Rulemaking and Notice of Inquiry, and they should have a separate and distinct heading designating them as responses to the IRFA. The Commission's Consumer and Governmental Affairs Bureau, Reference Information

[243] Consumer Tech. Ass'n, *Smart Policy to Secure our Smart Future: How to Promote a Secure Internet of Things for Consumers* (Mar. 2021) (*CTA Cybersecurity White Paper*), https://www.cta.tech/Resources/Newsroom/Media-Releases/2021/March/IOT-Device-Security-White-Paper-Release.

[244] *CTA Cybersecurity White Paper*, at 2-3.

[245] *CTA Cybersecurity White Paper*, at 7-13.

[246] *Id.* at 8.

[247] Exec. Order No. 14028, *Executive Order on Improving the Nation's Cybersecurity*, 86 Fed. Reg. 26633, 26640-41, § 4(s)-(u) (May 17, 2021).

[248] *See* 5 U.S.C. § 603.

Center, will send a copy of this Notice of Proposed Rulemaking and Notice of Inquiry, including the IRFA, to the Chief Counsel for Advocacy of the Small Business Administration, in accordance with the RFA.[249]

105. *Paperwork Reduction Act.* This document contains proposed new or modified information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and the Office of Management and Budget (OMB) to comment on the information collection requirements contained in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104-13.[250] In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198,[251] we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.

106. *Ex Parte Rules – Permit but Disclose*. Pursuant to section 1.1200(a) of the Commission's rules,[252] this Notice of Proposed Rulemaking and Notice of Inquiry shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[253] Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with rule 1.1206(b). In proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (e.g., .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

107. *Comment Period and Filing Procedures.* Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. All filings must refer to ET Docket No. 21-232 and EA Docket No. 21-233.

- Electronic filers: Comments may be filed electronically using the Internet by accessing the Commission's Electronic Comment Filing System (ECFS): https://www.fcc.gov/ecfs. *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).

- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing.

[249] *See* 5 U.S.C. § 603(a).

[250] 44 U.S.C. §§ 3501-3520.

[251] *See* 44 U.S.C. § 3506(c)(4),

[252] 47 CFR § 1.1200(a).

[253] 47 CFR §§ 1.1200 *et seq.*

- Filings can be sent by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.
- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
- U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street NE, Washington, DC 20554.

- Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19. *See* FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy, Public Notice, DA 20-304 (March 19, 2020). https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy.

108. People with Disabilities: To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer and Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (tty).

109. Availability of Documents: Comments, reply comments, and *ex parte* submissions will be publicly available online via ECFS.[254] When the FCC Headquarters reopens to the public, these documents will also be available for public inspection during regular business hours in the FCC Reference Center, Federal Communications Commission, 45 L Street NE, Washington, DC 20554.

110. *Further Information*. For further information, contact Jamie Coleman of the Office of Engineering and Technology, at 202-418-2705 or Jamie.coleman@fcc.gov.

V. ORDERING CLAUSES

111. Accordingly, IT IS ORDERED that, pursuant to the authority found in sections 4(i), 301, 302, 303, 309(j), 312, and 316 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 301, 302, 303, 309(j), 312 and 316, and section 1.411 of the Commission's Rules, 47 CFR § 1.411, that this Notice of Proposed Rulemaking and Notice of Inquiry IS HEREBY ADOPTED.

112. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this Notice of Proposed Rulemaking and Notice of Inquiry, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch

[254] Documents will generally be available electronically in ASCII, Microsoft Word, and/or Adobe Acrobat.

Secretary

APPENDIX A

Proposed Rules

For the reasons set forth in the preamble, the Federal Communications Commission amends part 2 of Title 47 of the Code of Federal Regulations as follows:

Part 2 — FREQUENCY ALLOCATIONS AND RADIO TREATY MATTERS; GENERAL RULES AND REGULATIONS

1. The authority citation for part 2 continues to read as follows:

Authority: 47 U.S.C. 154, 302a, 303, and 336, unless otherwise noted.

2. Add section 2.903 to subpart J to read as follows:

§ 2.903 Prohibition on equipment authorization of equipment on the Covered List.

Any equipment on the Covered List, as defined in § 1.50002 of this chapter, is prohibited from obtaining an equipment authorization under this subpart. This includes:

(a) Equipment subject to certification procedures: Telecommunication Certification Bodies and the Federal Communications Commission are prohibited from issuing a certification under this subpart for any equipment on the Covered List; and

(b) Equipment subject to Supplier's Declaration of Conformity procedures: Responsible parties, as defined in § 2.909 of this part, associated with the Supplier's Declaration of Conformity are prohibited from issuing a Supplier's Declaration of Conformity for any equipment on the Covered List.

APPENDIX B

INITIAL REGULATORY FLEXIBILITY ANALYSIS

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[255] the Commission has prepared this present Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities by the policies and rules proposed in this Notice of Proposed Rulemaking (Notice). Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments on the Notice provided in the item. The Commission will send a copy of the Notice, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).[256] In addition, the Notice and IRFA (or summaries thereof) will be published in the Federal Register.[257]

A. Need for, and Objectives of, the Proposed Rules

2. In this Notice of Proposed Rulemaking, we propose prohibiting the authorization of any equipment on the list of equipment and services (Covered List) that the Commission maintains pursuant to the Secure and Trusted Communications Networks Act of 2019.[258] Such equipment has been found to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons. We also seek comment on whether and under what circumstances we should revoke any existing authorizations of such "covered" communications equipment. Finally, we invite comment on whether we should require additional certifications relating to national security from applicants who wish to participate in Commission auctions.

B. Legal Basis

3. The proposed action is taken under authority found in sections 4(i), 301, 302, 303, 309(j), 312, and 316 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 301, 302, 303, 309(j), 312 and 316; and section 1.411 of the Commission's Rules, 47 CFR § 1.411.

C. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply

4. [Forthcoming]

D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

5. [Forthcoming]

E. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

6. [Forthcoming]

---

[255] *See* 5 U.S.C. § 603. The RFA, *see* 5 U.S.C. §§ 601–612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[256] *See* 5 U.S.C. § 603(a).

[257] *See id.*

[258] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609) (Secure Networks Act). The Commission's Public Safety and Homeland Security Bureau (PSHSB) maintains the list at https://www.fcc.gov/supplychain/coveredlist.

F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules

7. None.