6712-01

This document is scheduled to be published in the Federal Register on 08/19/2021 and available online at **federalregister.gov/d/2021-16087**, and on **govinfo.gov**

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 2

[ET Docket No. 21-232, EA Docket No. 21-233; FCC 21-73; FR ID 39556]

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

AGENCY: Federal Communications Commission.

ACTION: Request for comments.

SUMMARY: The Commission seeks comment on how to 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.

DATES: Comments are due on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**; reply comments are due on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by ET Docket No. 21-232, by any of the following methods:

- Federal Communications Commission's Web Site: http://apps.fcc.gov/ecfs/. Follow the instructions for submitting comments.
- Mail: Filings can be sent by hand or messenger delivery, 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.

For detailed instructions for submitting comments and additional information on the rulemaking process, see the SUPPLEMENTARY INFORMATION section of this document.

FOR FURTHER INFORMATION CONTACT: Jamie Coleman Office of Engineering and Technology, 202-418-2705, Jamie.Coleman@fcc.gov.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Notice of Inquiry (NOI), that is part of ET Docket No. 21-232, EA Docket No. 21-233, FCC 21-73, that was adopted and released June 17, 2021. The full text of this document is available by downloading the text from the

Commission's web site at: https://www.fcc.gov/document/equipment-authorization-and-competitive-bidding-supply-chain-nprm. When the FCC Headquarters reopens to the public, the full text of this document will also be available for public inspection and copying during regular business hours in the FCC Reference Center, 45 L Street NE, Washington, DC 20554. Alternative formats are available for people with disabilities (braille, large print, electronic files, audio format), by sending an email to fcc504@fcc.gov or calling the Consumer and Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (TTY).

Comment Filing Procedures

Pursuant to §§ 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. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).

- Electronic Filers: Comments may be filed electronically using the Internet by accessing the ECFS: http://apps.fcc.gov/ecfs/.
- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing.
- 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.

Initial Paperwork Reduction Act of 1995 Analysis

This document does not contain proposed information collection requirements subject to the Paperwork Reduction Act of 1995, Public Law 104-13. In addition, therefore, it does not contain any proposed information collection burden for small business concerns with fewer than 25 employees, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, see 44 U.S.C. 3506(c)(4).

***Ex Parte* Rules—Permit-But-Disclose**

The proceeding this NOI initiates shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules, 47 CFR 1.1200 *et seq*. 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.

Synopsis

The Commission adopted this Notice of Inquiry (NOI) in conjunction with a Notice of Proposed Rulemaking, ET Docket No. 21-232, EA Docket No. 21-233, FCC 21-73, in which it proposes direct action to limit the presence of untrusted equipment and services in U.S. networks. The Commission believes that ensuring continued U.S. leadership requires that the Commission also explore opportunities to spur trustworthy innovation for more secure equipment. In this NOI, the Commission seeks 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.

The development and implementation of effective cybersecurity practices requires the continued cooperation and participation of all stakeholders. In this regard, the Commission observes 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. 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 consists of "voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk." *See* Nat'l Inst. of Standards & Tech., *Cybersecurity Framework: New to Framework* (last updated Sept. 23, 2020), https://www.nist.gov/cyberframework/new-framework. 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. *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. In addition, among

other organizations, the Federal Trade Commission has been active in cybersecurity matters for years, bringing multiple enforcement actions against firms for having poor cybersecurity practices and offering cybersecurity guidance for Internet of Things (IoT) devices as early as 2015. 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. Further, industry trade groups, including CTIA–The Wireless Association, GSMA, the ioXt Alliance, and TIA 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. *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/.

More recently, NIST has developed a Cybersecurity for 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." 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. Devices that operate as part of the 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.

This Cybersecurity for IoT program has produced multiple reports, but perhaps most notable is Internal Report 8259, released in May 2020. 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. 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." *Id.* 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 process.

The Commission seeks comment on how it 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? Are there other technologies or cybersecurity methods that mitigate security risks (e.g., RF fingerprinting or some other method)? What, if anything, should the Commission be doing to encourage development and adoption of such technologies or methods? 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.

Even with broad adoption of industry best practices and standards, some equipment sold in the United States may lack appropriate security protections. What is the role of retailers in voluntarily limiting the sale of such equipment? How can retailers educate consumers about the importance of security protections for their devices? The Commission also seeks to understand developments in international standards-setting bodies What is the status of international standards-setting that could be relevant to supply chain security, and what can the FCC do to encourage action by international standards-setting bodies and participation by American companies in their efforts?

The Commission observes 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. 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. In this white paper, CTA encourages public-private partnerships to develop and deploy risk-based approaches to cybersecurity, and argues that "neither the new Administration nor Congress should embrace rules, product labels or certification regimes for consumer IoT." 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." The Commission seeks 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?

The Commission recognizes that consideration of how to incentivize cybersecurity best practices through the 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. Exec. Order No. 14028, *Executive Order on Improving the Nation's Cybersecurity*, 86 Fed. Reg. 26633, 26640-41, § 4(s)-(u) (May 17, 2021). While the Director of NIST has not yet identified the agencies that will participate in the forthcoming IoT cybersecurity labeling program, the Commission seeks comment on whether the Commission can support these efforts, either directly or indirectly. If so, how?

Legal authority

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." 47 U.S.C. 151. The Commission tentatively concludes 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." 47 U.S.C. 154(i). The Commission believes 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, 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, the duties under the National Environmental Policy Act to regulate human RF exposure, the Commission's duty to ensure that mobile handsets are compatible with hearing aids, and the 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. The Commission believes that these processes can and should also serve the purpose of fulfilling other Commission responsibilities under the Secure Networks Act, and the Commission seeks comment on that issue.

The Commission also believes that other authorities in the Communications Act of 1934, as amended, provide authority for the Commission to rely on for potential 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. *See Equipment Authorization of RF Devices*, Docket No. 19356, Report and Order, 39 Fed. Reg. 5912, 5912, para. 2 (1970). 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." 47 U.S.C. 302(a)(1). Regulations that the Commission adopts 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." 47 U.S.C. 302(a)(2). 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. The

Commission seeks comment on the scope of the authority to rely on such rules to effectuate other public interest responsibilities, including the Commission's section 303(e) authority to "[r]egulate the kind of apparatus to be used with respect to its external effects." 47 U.S.C. 303(e).

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. The Commission seeks comment on this tentative conclusion.

The Commission also seeks comment on a potential alternative basis for such security rules. The Communications Assistance for Law Enforcement Act (CALEA) includes security requirements that apply directly to equipment intended for use by providers of telecommunications services. 47 U.S.C. 1001-1010. 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," (47 U.S.C. 1004) 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. *Supply Chain First Report and Order*, 34 FCC Rcd at 11436-37, paras. 35-36. The Commission is required to prescribe rules necessary to implement CALEA's requirements. 47 U.S.C. 229.

As noted above, the Commission believes it has ancillary authority under section 4(i) of the Act to consider revisions to its part 2 rules as reasonably necessary to the effective enforcement of the Secure Networks Act. The Commission also tentatively concludes that such rules would be consistent with the Commission's 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 the 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. The Commission seeks comment on this reasoning as well. The Commission also seeks comment on any

other sources of authority for the Commission to propose rules as a result of this Notice of Inquiry.

FEDERAL COMMUNICATIONS COMMISSION

Marlene Dortch,
Secretary.

[FR Doc. 2021-16087 Filed: 8/18/2021 8:45 am; Publication Date: 8/19/2021]