[6712-01]

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 8

[PS Docket Nos. 23-239; FR ID 210016]

Cybersecurity Labeling for Internet of Things

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: In this document, the Federal Communications Commission (FCC or Commission) adopts a voluntary cybersecurity labeling program for wireless consumer Internet of Things, or IoT, products. The final rule also requires applicant manufacturers to make certain disclosures related to their product(s) for authorization to use the FCC IoT Label. This is a summary of the Further Notice of Proposed Rulemaking (Further Notice), in which the Commission proposes rules on additional national security declarations for the IoT labeling program. These requirements would further help consumers make safer purchasing decisions, raise consumer confidence regarding the cybersecurity of the IoT products they buy, and encourage manufacturers to develop IoT products with security-by-design principles in mind.

DATES: Comments are due on or before **[30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]** and reply comments are due on or before **[60 DAYS AFTER DATE OF PUBLICATION.]** Written comments on the Paperwork Reduction Act proposed information collection requirements must be submitted by the public, Office of Management and Budget (OMB), and other interested parties on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].**

ADDRESSES: You may submit comments, identified by PS Docket No. 23-239, by any of the following methods:

- Federal Communications Commission's website: https://www.apps.fcc.gov/ecfs/. Follow the instructions for submitting comments.

- Mail: Parties who choose to file by paper must file an original and one copy of each filing. If more than one docket or rulemaking number appears in the caption of this proceeding, filers must submit two additional copies for each additional docket or rulemaking number. 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.
- 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 & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (TTY).

FOR FURTHER INFORMATION CONTACT: For further information regarding these proposed rules, please contact Zoe Li, Attorney Advisor, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-2490, or by email to Zoe.Li@fcc.gov.

For additional information concerning the Paperwork Reduction Act information collection requirements contained in this document, send an email to PRA@fcc.gov or contact Nicole

Ongele, Office of Managing Director, Performance Evaluation and Records Management, 202-418-2991, or by email to PRA@fcc.gov.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Further Notice of Proposed Rulemaking (FNPRM), FCC 24-26, adopted March 14, 2024, and released March 15, 2024. The full text of this document is available by downloading the text from the Commission's website at: https://docs.fcc.gov/public/attachments/FCC-24-26A1.pdf.

SYNOPSIS

Further Notice of Proposed Rulemaking

1. In this FNPRM, we seek comment on additional declarations intended to provide consumers with assurances that the products bearing the FCC IoT Label do not contain hidden vulnerabilities from high-risk countries, that the data collected by the products does not sit within or transit high-risk countries, and that the products cannot be remotely controlled by servers located within high-risk countries. Specifically, we seek comment on whether we should require manufacturers to disclose to the Commission whether firmware and/or software were developed and manufactured in a "high-risk country," as well as where firmware and software updates will be developed and deployed from. We also seek comment on whether to require manufacturers to disclose to consumers in the registry whether firmware and/or software were developed and manufactured in a "high-risk country," as well as where firmware and software updates will be developed and deployed from. We propose to include as high-risk countries those foreign adversary countries defined by the Department of Commerce in 15 CFR 7.4. Are there other sources that the Commission should consider for identifying high-risk countries? Specifically, we seek comment on whether to require the applicant seeking to use the FCC IoT Label to make one of the following declarations under penalty of perjury to accompany its application to use the label:

a. No software or software update or part of any software or software update that runs on or controls the product was or will be developed or deployed from within a country on the Secretary

of Commerce's list of high-risk countries, except that this commitment does not apply to the origin of open-source contributions not paid for directly or indirectly by us or our direct or indirect partners in offering this product; or

b. This device runs, or due to future software updates might run, software developed within the Secretary of Commerce's list of high-risk country or countries. Applicant is not aware of any backdoors or other sabotage, or any reason to believe that there is a particular heightened risk for such backdoors or sabotage relative other software developed within such a country, but we inform purchasers and users that the Department of Commerce has designated high-risk country or countries as jurisdictions whose conduct is significantly adverse to the national security of the United States or security and safety of United States persons.

2. We also seek comment on requiring manufacturers to disclose to the Commission whether the data collected by the product is stored in or transits a high-risk country or countries. We also seek comment on whether to require manufacturers to disclose to consumers in the registry whether the data collected by the product is stored in or transits a country or countries that are known to pose a national security risk to the United States. Does the manufacturer have sufficient knowledge of the data collected by the device to know where the servers hosting the collected data are located or where the servers remotely controlling the device will be located? Is it possible for the location of stored data to be changed without the manufacturer's knowledge? Are there other factors that would impact the manufacturer's ability to make these declarations. Specifically, we seek comment on requiring the applicant seeking to use the FCC IoT Label to make one of the following declarations under penalty of perjury to accompany its application to use the label:

> a. No customer data collected by this product will be sent to servers located on the Department of Commerce's list of high-risk countries, defined at 15 CFR 7.4 or any successor regulation. No servers that remotely control the device will be located in such a country; or

b. Customer data collected by this product will be sent to servers located in a high-risk country or countries. We inform purchasers and users that the Secretary of Commerce has designated high-risk country or countries as jurisdictions whose conduct is significantly adverse to the national security of the United States or security and safety of United States persons.

3. If a manufacturer must disclose one of these exposures or potential exposures to a high-risk country, should it have to disclose additional information as well? Should it have to disclose the identity of the high-risk country or countries? Should it have to disclose the specific hardware or software components or server activities that did, will, or could originate from or take place in those countries? How could such disclosures help purchasers make informed decisions about product acquisitions? And what burdens would such additional disclosures place on manufacturers? Should we require manufacturers to include this information in the registry to inform consumers of these issues?

4. Alternatively, should the fact that software or firmware originates from such countries, that data will be stored in such countries, or that products can be remotely controlled by servers within such countries, make products ineligible for the label altogether? Are there certain product components, such as cellular interface modules, that pose elevated risks for which such a prohibition might specifically be warranted?

5. With respect to these declarations proposed to require the manufacturer to inform the Commission, would such information provide meaning to consumers? Should we require manufacturers to include this information in the registry to inform consumers of these issues? How would manufacturers inform users who are not purchasers? In addition, we seek comment on the possible costs and benefits of requiring any additional language in the relevant product's registry page. Should they encompass some or all of the same representations made in an application for authorization to use the FCC label, or should they be different or additional? Can such representations be made not just for the benefit of the purchaser or user, but also extend to

any third parties who may be impacted by a security vulnerability in a labeled product attributable to a failure of the manufacturer, and what would the practical or legal implications of that be? How might this influence manufacturer participation in the program? Could the federal Magnuson-Moss Act be an additional legal overlay here, as well? How should those state and federal laws inform whether and how the Commission requires manufacturer or seller representations in the product's registry page?

Procedural Matters

6. **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. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, see 44 U.S.C. 3506(c)(4), we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees. The Bureau does not believe that the new or modified information collection requirements we adopt here will be unduly burdensome on small businesses.

7. In this present document, we have assessed the effects of the operational framework for a voluntary IoT cybersecurity labeling program. Since the IoT Labeling Program is voluntary, small entities who do not participate in the IoT Labeling Program will not be subject to any new or modified reporting, recordkeeping, or other compliance obligations. Small entities that choose to participate in the IoT Labeling Program by seeking authority to affix the Cyber Trust Mark on their products will incur recordkeeping and reporting as well as other obligations that are necessary to test their IoT products to demonstrate compliance with the requirements we adopt today. We find that, for the Cyber Trust Mark to have meaning for consumers, the requirements for an IoT product to receive the Cyber Trust Mark must be uniform for both small

businesses and other entities. Thus, the Commission continues to maintain the view we expressed in the IoT Labeling NPRM, that the significance of mark integrity, and building confidence among consumers that devices and products containing the Cyber Trust Mark label can be trusted to be cyber secure, necessitates adherence by all entities participating in the IoT Labeling Program to the same rules regardless of size.

8. Regulatory Flexibility Act. The Regulatory Flexibility Act of 1980, as amended (RFA), requires that an agency prepare a regulatory flexibility analysis for notice and comment rulemakings, unless the agency certifies that "the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities." Accordingly, we have prepared a Final Regulatory Flexibility Analysis (FRFA) concerning the possible impact of the rule changes contained in this Report and Order on small entities. The FRFA is set forth in Appendix B of the FCC's Report and Order and Further Notice of Proposed Rulemaking, FCC 24-26, adopted March 14, 2024, at this link: https://docs.fcc.gov/public/attachments/FCC-24-26A1.pdf.

9. We have also prepared an Initial Regulatory Flexibility Analysis (IRFA) concerning the potential impact of rule and policy change proposals on small entities in the FNPRM. The IRFA is set forth in Appendix C of the FCC's Report and Order and Further Notice of Proposed Rulemaking, FCC 24-26, adopted March 14, 2024, at this link: https://docs.fcc.gov/public/attachments/FCC-24-26A1.pdf. The Commission invites the general public, in particular small businesses, to comment on the IRFA. Comments must be filed by the deadlines for comments on the FNPRM indicated on the first page of this document and must have a separate and distinct heading designating them as responses to the IRFA.

10. OPEN Government Data Act. The OPEN Government Data Act requires agencies to make "public data assets" available under an open license and as "open Government data assets," i.e., in machine-readable, open format, unencumbered by use restrictions other than intellectual property rights, and based on an open standard that is maintained by a standards organization. This requirement is to be implemented "in accordance with guidance by the Director" of the

OMB. The term "public data asset" means "a data asset, or part thereof, maintained by the Federal Government that has been, or may be, released to the public, including any data asset, or part thereof, subject to disclosure under the Freedom of Information Act (FOIA)." A "data asset" is "a collection of data elements or data sets that may be grouped together," and "data" is "recorded information, regardless of form or the media on which the data is recorded." We delegate authority, including the authority to adopt rules, to the Bureau, in consultation with the agency's Chief Data Officer and after seeking public comment to the extent it deems appropriate, to determine whether to make publicly available any data assets maintained or created by the Commission within the meaning of the OPEN Government Act pursuant to the rules adopted herein, and if so, to determine when and to what extent such information should be made publicly available. Such data assets may include assets maintained by a CLA or other third-party, to the extent the Commission's control or direction over those assets may bring them within the scope of the OPEN Government Act, as interpreted in the light of guidance to be issued by OMB.[1] In doing so, the Bureau shall take into account the extent to which such data assets are subject to disclosure under the FOIA.

11. Ex Parte Rules – Permit-But-Disclose. The proceeding this Further Notice of Proposed Rulemaking initiates shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's ex parte rules. 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

[1] OMB has not yet issued final guidance.

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 section 1.1206(b) of the Commission's rules. In proceedings governed by §1.49(f) of the Commission's rules 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.

12. **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).

13. **Providing Accountability Through Transparency Act**. Consistent with the Providing Accountability Through Transparency Act, Pub. Law 118-9, a summary of this document will be available on https://www.fcc.gov/proposed-rulemakings.

Legal Basis

14. The proposed action is authorized pursuant to sections 1, 2, 4(i), 4(n), 302, 303(r), 312, 333, and 503, of the Communications Act of 1934, as amended, 47 U.S.C. 151, 152, 154(i), 154(n), 302a, 303(r), 312, 333, 503; and the IoT Cybersecurity Improvement Act of 2020, 15 U.S.C. 278g-3a through 278g-3e.

Initial Regulatory Flexibility Analysis

15. An Initial Regulatory Flexibility Act (IRFA) Analysis for the rules proposed in the FNPRM was prepared and can be found as Exhibit B of the FCC's Second Report and Order and Further Notice of Proposed Rulemaking, FCC 24-5, adopted January 26, 2024, at this link: https://docs.fcc.gov/public/attachments/FCC-24-26A1.pdf.

FEDERAL COMMUNICATIONS COMMISSION

Katura Jackson,
Federal Register Liaison Officer.

[FR Doc. 2024-06249 Filed: 3/22/2024 8:45 am; Publication Date: 3/25/2024]