February 22, 2024

FCC FACT SHEET[*]

Cybersecurity Labeling for Internet of Things

Report and Order PS Docket No. 23-239

Background:

Consumers rely on Internet-connected products to help manage many aspects of day-to-day life, including home safety, health, recreation, and personal convenience. With this convenience, however, comes risk. Internet of Things (IoT) products are susceptible to a wide range of relatively common security vulnerabilities that are increasingly exploited by cybercriminals who are invading people's privacy and threatening national security. Consumers who purchase an IoT product that bears an FCC Label can be assured that their product meets the cybersecurity standards of the IoT Labeling Program, which in turn will strengthen the chain of connected IoT products in their own homes and as part of a larger national IoT ecosystem.

What the Order Does:

- The Order would establish a voluntary IoT cybersecurity labeling program based on the criteria developed by the National Institute for Standards and Technology. The labeling program would help consumers make better purchasing decisions, raise consumer confidence with regard to the cybersecurity of the IoT products they buy to use in their homes, and encourage manufacturers to develop IoT products with security-by-design principles in mind.
- The FCC Label would include the U.S. Cyber Trust Mark and a QR Code linking to a product registry. The registry would display consumer-friendly information about the security of products bearing the Cyber Trust Mark.
- The program would initially focus on wireless consumer IoT products, which includes the IoT devices and additional product components that are needed for a consumer to use the IoT product beyond basic operational features. This might include, for example, a smart speaker, doorbell or shopping device and the apps used to control them.
- While this labeling program is administered by the FCC, close collaboration between the federal government, industry, and other stakeholders will be vital to ensuring its success.
- Cybersecurity Labeling Administrators (CLAs), including a Lead Administrator selected by the Commission, would help the Commission stand up the program and be responsible for day-to-day program management. CLAs would receive, review, and approve/deny applications from manufacturers that want authorization to use the FCC Label. Each application would be supported by testing conducted by an accredited lab demonstrating the product complies with the FCC's program standards.
- The success of this program would rely on a robust consumer education campaign with shared responsibilities among the government, manufacturers, retailers, industry, and other cybersecurity groups to promote label recognition, brand trust, and transparency.

[*] 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 PS Docket No. 23-239, 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	)	
	)	
Cybersecurity Labeling for Internet of Things	)	PS Docket No. 23-239
	)	

REPORT AND ORDER[*]

Adopted: [ ] **Released: [ ]**

By the Commission:

TABLE OF CONTENTS

Heading Paragraph #

I. INTRODUCTION 2
II. BACKGROUND 4
  A. The Internet of Things (IoT) Landscape 4
  B. Public and Private IoT Security Efforts 6
III. REPORT AND ORDER 12
  A. Voluntary IoT Labeling Program 12
  B. Eligible Devices or Products 15
  C. Oversight and Management of the IoT Labeling Program 41
    1. Fostering Close Public-Private Collaboration 41
    2. Cybersecurity Label Administrators (CLAs) 48
    3. Responsibilities of the Lead Administrator and CLAs 52
    4. Selecting CLAs and Revoking Authority to Grant Applications to Use the FCC IoT Label 60
  D. CyberLABs, CLA-Run Labs, and In-House Testing Labs 66
  E. Two-Step Process for Obtaining Authority to Use the FCC IoT Label 82
    1. Product Testing by an Accredited and Recognized Lab 83
    2. Filing an Application with a CLA 88
  F. Consumer IoT Product Cybersecurity Criteria and Standards 97
  G. The FCC IoT Label (Cyber Trust Mark and QR Code) 107

[*] This document has been circulated for tentative consideration by the Commission at its March 14, 2024 open meeting. The issues referenced in this document and the Commission's ultimate resolution of those issues remain under consideration and subject to change. This document does not constitute any official action by the Commission. However, the Chairwoman has determined that, in the interest of promoting the public's ability to understand the nature and scope of issues under consideration, the public interest would be served by making this document publicly available. The FCC'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.

H. Registry 112
I. Continuing Obligations of Entities Authorized to Use the FCC IoT Label 123
J. Audits, Post-Market Surveillance, and Enforcement 126
K. International Reciprocal Recognition of the Cyber Trust Mark 133
L. Consumer Education 137
M. Cost/Benefit Analysis 143
IV. LEGAL AUTHORITY 152
V. PROCEDURAL MATTERS 162
VI. ORDERING CLAUSES 169
APPENDIX A – Final Rules
APPENDIX B – Final Regulatory Flexibility Analysis

I. INTRODUCTION

1. Consumers rely heavily on Internet-connected products to help them manage many aspects of day-to-day life, including home safety, health, recreation, and personal convenience. With this convenience, however, comes risk. Internet of Things (IoT) products are susceptible to a wide range of relatively common security vulnerabilities that are increasingly exploited by cybercriminals who are invading people's privacy and threatening national security. With this Report and Order (Order), the Commission takes prompt and decisive measures to strengthen the nation's cybersecurity posture by adopting a voluntary cybersecurity labeling program for wireless Internet of Things products.[1] The Commission's IoT Labeling Program will provide consumers with an easy-to-understand and quickly recognizable FCC IoT Label that includes the U.S. government certification mark (referred to as the Cyber Trust Mark) that provides assurances regarding the baseline cybersecurity of an IoT product, together with a QR code that directs consumers to a registry with specific information about the product. Consumers who purchase an IoT product that bears the FCC IoT Label can be assured that their product meets the minimum cybersecurity standards of the IoT Labeling Program, which in turn will strengthen the chain of connected IoT products in their own homes and as part of a larger national IoT ecosystem. Today's Order will help consumers make better purchasing decisions, raise consumer confidence with regard to the cybersecurity of the IoT products they buy to use in their homes and their lives, and encourage manufacturers of IoT products to develop products with security-by-design principles in mind.[2]

2. In the following Order, we set forth the framework by which the IoT Labeling Program will operate. We focus the IoT Labeling Program initially on IoT "products," which we define to include one or more IoT devices and additional product components necessary to use the IoT device beyond basic operational features. Recognizing that a successful voluntary IoT Labeling Program will require close partnership and collaboration between industry, the federal government, and other stakeholders, we adopt an administrative framework for the IoT Labeling Program that capitalizes on the existing public, private, and academic sector work in this space, while ensuring the integrity of the IoT Labeling Program through oversight by the Commission.

[1] *See Cybersecurity Labeling for Internet of Things*, PS Docket No. 23-239, FCC 23-65, Notice of Proposed Rulemaking (Aug. 10, 2023) (*IoT Labeling NPRM*); *see also* Exec. Order No. 14028, *Improving the Nation's Cybersecurity*, 86 Fed. Reg. 26633 (May 12, 2021) (*IoT Executive Order*). The IoT Labeling Program has also been referred to as the "U.S. Cyber Trust Mark program." *See* Press Release, White House, Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers (July 18, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/ [https://perma.cc/BR9A-JU59].

[2] See Cybersecurity & Infrastructure Security Agency, *Secure-by-Design, Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software*, (Oct. 25, 2023), https://www.cisa.gov/resources-tools/resources/secure-by-design [https://perma.cc/8NPX-YR4A] (urging software manufacturers "to take urgent steps necessary to ship products that are secure by design and revamp their design and development programs to permit only secure by design products to be shipped to customers").

II. BACKGROUND

A. The Internet of Things (IoT) Landscape

3. Consumer IoT products communicate over wired and wireless networks using a varying array of technologies, each of which presents its own set of security challenges.[3] In August 2023, the Commission adopted a Notice of Proposed Rulemaking (*IoT Labeling NPRM*) proposing a voluntary program for IoT labeling that would provide consumers with easily understood, accessible information on the relative security of an IoT device or product.[4] The record received in response to the *IoT Labeling NPRM* reflects that cybersecurity threats to IoT products present a significant risk, as nefarious actors try to take advantage of insecure consumer IoT products. For example, Distributed Denial of Service (DDoS) attacks using exploited IoT products continue to increase, "with DDoS attacks 'originating from insecure IoT devices increase[ing] five-fold' over 2022 and 2023."[5] These attacks can disrupt services that consumers rely on.[6] As noted in the record, all types of IoT consumer products are subject to attack, with commenters explaining that "[o]nce-harmless devices like printers and baby monitors can be conscripted into botnets that conduct massive [DDoS] attacks."[7] Some IoT products have even shipped with malware in them.[8] Further, consumer IoT products may face attacks not readily anticipated by consumers, with Consumer Reports explaining how IoT products can be manipulated by hackers using electromagnetic interference (EMI) "to duplicate sounds that can lead to a hacker activating a smart speaker."[9] The record cites the impacts insecure IoT devices have on consumers, highlighting that "nearly one-quarter of users with 20 or more devices in a household have experienced two or more data security breaches in the past year."[10]

4. Consumers are concerned about the security of their IoT products, but they generally do not have access to convenient information on the security risk of these products prior to purchasing one. As highlighted by the Electronic Privacy Information Center (EPIC), readily available security information for consumers is lacking before purchasing IoT products, because the security and privacy information "is often buried within in-box instruction manuals consumers cannot access until after

[3] *See Cybersecurity Labeling for Internet of Things*, PS Docket No. 23-239, FCC 23-65, Notice of Proposed Rulemaking, para. 3 (2023) (*IoT Labeling NPRM*).

[4] *IoT Labeling NPRM* at 1-2, paras. 1-2.

[5] Comcast Corporation Comments at 9 (Comcast) (citing Press Release, Nokia, Nokia Threat Intelligence Report Finds Malicious IoT Botnet Activity Has Sharply Increased (June 7, 2023), https://www.nokia.com/about-us/news/releases/2023/06/07/nokia-threat-intelligence-report-finds-malicious-iot-botnet-activity-has-sharply-increased/#:~:text=Espoo%2C%20Finland%20%E2%80%93%20The%20latest%20Nokia,fivefold%20over%20the%20past%20year%2C [https://perma.cc/5KHF-CM86]).

[6] *See, e.g.*, Jake Frankenfield, *Denial-of-Service (DoS) Attack: Examples and Common Targets*, Investopedia (May 24, 2023), https://www.investopedia.com/terms/d/denial-service-attack-dos.asp [https://perma.cc/9AK9-ND28] ("In October 2016, a DDoS attack was carried out on a domain name system (DNS) provider, Dyn… The attack on Dyn flooded its servers with overwhelming traffic, creating a massive web outage and shutting down over 80 websites, including major sites like Twitter (now X), Amazon, Spotify, Airbnb, PayPal, and Netflix.").

[7] CTA Comments at 2.

[8] Sead Fadilpašić, *These Popular Android TV Boxes are Reportedly Shipping Laced with Malware*, techradar (May 21, 2023), https://www.techradar.com/news/these-popular-android-tv-boxes-are-laced-with-malware [https://perma.cc/32JX-R8T5].

[9] Consumer Reports Comments at 4; *see also* Forrest McKee Comments at 1 (describing the "“Near Ultrasonic Inaudible Trojan Attack," which utilizes audio signals between 16 and 22 kHz, typically beyond the average adult's hearing range, to discreetly issue malicious commands to devices.").

[10] NTCA – The Rural Broadband Association Comments at 2 (NTCA) (citing Susanne Hupfer, Michael Steinhart, *Shiny New Devices May Bring Joy, But Who's Protecting Consumer Data?*, Deloitte Insights (Jan. 23, 2023)).

purchase."[11] Further, research conducted by Consumer Reports indicates that more than half of consumers surveyed were concerned about the information collected by connected devices.[12] Consumer Reports research also found that more than half of surveyed consumers did not feel informed about the security of the data collected by IoT devices.[13] A majority of consumers surveyed by Consumer Reports felt that the data collected and with whom it was shared was important for them to know, and that it was the responsibility of manufacturers to provide this information to the consumer.[14] Consumer Reports also found widespread consumer uncertainty and distrust on topics such as the length of time the manufacturer would provide software updates and whether the company stored consumer information.[15] Consumer Reports concluded that "[c]onsumers clearly value information from manufacturers as to how their data gets used and stored, how long a product will receive security updates and how good a manufacturer's security practices are, but have no consistent way to find that information, and aren't sure if the info provided is trustworthy."[16] Our IoT Labeling Program is intended to provide consumers with that missing piece.

B. Public and Private IoT Security Efforts

5. As the Commission observed in the *IoT Labeling NPRM*, significant work has already been conducted in the realm of IoT cybersecurity.[17] Because the context of the Commission's action in

[11] Electronic Privacy Information Center (EPIC) Reply at 5.

[12] Letter from Stacey Higginbotham, Policy Fellow, Consumer Reports, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 23-239, Attach. *CR IoT Security Label Summer Research* at 4 (filed Dec. 13, 2023) (*Consumer Reports Summer Research*).

[13] *Consumer Reports Summer Research* at 4.

[14] *Id.* at 4-5.

[15] *Id.* at 5-6.

[16] *Id.* at 8.

[17] We observe that the National Institute of Standards and Technology (NIST) issued several guidelines on cybersecurity for Internet-connected devices, stressing an engineering-based approach that builds security systems directly into IoT technology. *See*, NIST, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure System, NIST Special Pub. 800-160 (2016), https://doi.org/10.6028/NIST.SP.800-160 [https://perma.cc/4ASG-MQB2]; *see also* NIST, NISTIR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers at 15 (2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf [https://perma.cc/82CX-WXQ7]. The Department of Homeland Security (DHS) also previously released its own cybersecurity policy for IoT devices, delineating six strategic principles that it believes will help stakeholders stop unauthorized intruders from tampering with connected devices. *See* U.S. Dept. of Homeland Security, *Strategic Principles for Securing the Internet of Things (IoT)*, Version 1.0 (Nov. 15, 2016), https://www.dhs.gov/securingtheIoT [https://perma.cc/GG86-4UCH]. NIST and the National Telecommunications and Information Administration (NTIA) developed a risk management framework for addressing cybersecurity issues. *See* NIST, Framework for Improving Critical Infrastructure Cybersecurity (2014), https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf [https://perma.cc/C6M7-Z7V2]. The Communications Security, Reliability, and Interoperability Council IV (CSRIC IV) developed a segment-specific analysis of the application of the Cybersecurity Framework, as well as recommendations for voluntary efforts to address cybersecurity concerns. *See* CSRIC IV, Working Group 4, Cybersecurity Risk Management and Best Practices, Final Report (2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf [https://perma.cc/4P5E-5NKR]. In addition, the Commission's Technical Advisory Council issued its report on applying security to consumer IoT devices. *See* Federal Communications Commission Technical Advisory Council (FCC TAC), Cybersecurity Working Group, Technical Considerations White Paper (2015), https://transition.fcc.gov/oet/tac/tacdocs/reports/2015/FCC-TAC-Cyber-IoT-White-Paper-Rel1.1-2015.pdf [https://perma.cc/L3JD-FEVB]; *see also* Press Release, FTC, FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks (Jan. 27, 2015), https://www.ftc.gov/news-events/news/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices-address-

(continued….)

this Order is widely informed by government actions to date and the significant work of industry and academia, we reiterate here background information also found in the *IoT Labeling NPRM*, and highlight more recent and ongoing efforts to address IoT security labeling across both private and public sectors. We previously noted the progress of international efforts with respect to IoT labeling, such as the publication of an assessment methodology for IoT security provisions to assist assessors of IoT products for Singapore's Cybersecurity Labeling Scheme.[18] More recently, in September 2023, Japan announced its intention to "strengthen research collaboration" with the National Institute for Standards and Technology (NIST) and to work with the U.S. to ensure the interoperability of the IoT labeling scheme Japan is developing.[19] In addition, recognizing the importance of international cooperation to strengthen cybersecurity, the Cybersecurity and Infrastructure Security Agency (CISA) and thirteen international partners released guidance for software manufacturers to consider in making products secure by design.[20] CISA has also taken significant steps to provide consumers with tools to help them keep their families' online activities secure through CISA's Secure Our World program.[21] On January 30, 2024, the U.S. also entered into a Joint CyberSafe Products Action Plan with the European Union, aiming to advance technical cooperation in support of mutual recognition of their respective evolving IoT cybersecurity programs.[22]

6. The Commission further observed in the *IoT Labeling NPRM* the efforts to address IoT security across the U.S. government.[23] In May 2021, the *IoT Executive Order* emphasized the importance of IoT cybersecurity, noting the "persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy."[24] Securing the Internet of Things forms a significant pillar in the National Cybersecurity

consumer-privacy-security [https://perma.cc/M99B-JKJ3] (proposing privacy and cybersecurity best practices associated with IoT); U.S. Dept. of Health and Human Services, Radio Frequency Wireless Technology in Medical Devices: Guidance for Industry and Food and Drug Administration Staff (2013), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077272.pdf [https://perma.cc/WW47-7CYU] (guidance to the industry on considerations for the safe and effective development and use of RF technology in medical devices).

[18] *See* Cyber Security Agency of Singapore, Cybersecurity Labelling Scheme for IoT Publications No. 4, Assessment Methodology v.1.0, CCCSP-151-4 (2023), https://www.csa.gov.sg/docs/default-source/our-programmes/certification-and-labelling-scheme/cls/publications/-pub-ccc-sp-151-4-cls(iot)-assessment-methodology-v1.0.pdf?sfvrsn=7661147f_1 [https://perma.cc/CT9A-Z69E]. In October 2020, the Cyber Security Agency of Singapore launched its baseline cybersecurity requirements for IoT devices and products and updated its program effective September 22, 2023. Cyber Security Agency of Singapore, *Updates*, https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/updates [https://perma.cc/QP6R-WFUY] (last visited Feb. 13, 2024).

[19] Press Release, Ministry of Economy, Trade and Industry, Joint Statement of the Japan-U.S. Economic Policy Consultative Committee at 6 (Nov. 14, 2023), https://www.meti.go.jp/press/2023/11/20231116006/20231116006-1.pdf [https://perma.cc/GN7U-PYP4].

[20] Cybersecurity & Infrastructure Security Agency, *Secure by Design | Shifting the Balance of Cybersecurity Risk: principles and Approaches for Secure by Design Software* (Oct. 25, 2023), https://www.cisa.gov/resources-tools/resources/secure-by-design [https://perma.cc/NZ3Z-CMKF].

[21] Cybersecurity & Infrastructure Security Agency, *Secure Our World*, https://www.cisa.gov/secure-our-world [https://perma.cc/P2J7-M5YQ] (last visited Jan. 12, 2024).

[22] Press Release, European Commission, EU-US Joint Statement on CyberSafe Product Action Plan (Jan. 31, 2024), https://digital-strategy.ec.europa.eu/en/library/eu-us-joint-statement-cybersafe-products-action-plan [https://perma.cc/8D78-H97V].

[23] *IoT Labeling NPRM* at 5, para. 6.

[24] *IoT Executive Order* at 26633.

Strategy.[25] Pursuant to the "Modernizing Federal Government Cybersecurity" section of the *IoT Executive Order*,[26] the Office of Management and Budget (OMB), as part of its annual guidance on compliance with information security and privacy management requirements, directed federal agencies to inventory IoT devices and initiate a process to establish best practices for IoT security across the federal government.[27]

7. The Commission also observed the significant work of NIST,[28] including the *NIST Cybersecurity White Paper*[29] which details recommended criteria and potential labeling program approaches for cybersecurity labeling of consumer IoT products. The White Paper was informed by existing consumer product labeling programs, input provided by diverse stakeholders, public and private, gained from public workshops and comments filed in response to draft documents. The White Paper also relied heavily on the NIST Internal Report (NISTIR) 8259 family of documents (NISTIR 8259, NISTIR 8259A, and NISTIR 8259B),[30] which define the IoT cybersecurity capability core baseline. The core baseline is a set of foundational cybersecurity capabilities that manufacturers can use to identify the cybersecurity capabilities their customers may expect in IoT devices.[31]

8. In September 2022, NIST released the *Profile of the IoT Core Baseline for Consumer IoT Products (NISTIR 8425)*.[32] NISTIR 8425, which is built on NISTIR 8259A and NISTIR 8259B, identifies cybersecurity capabilities commonly needed for the consumer IoT sector and provides guidance for what consumers (including businesses as consumers) should consider when purchasing IoT products.[33] In NISTIR 8425, NIST describes a potential program that would educate the public on IoT cybersecurity capabilities, thereby allowing and enabling consumers in the marketplace to make informed

[25] White House, National Cybersecurity Strategy at 20 (2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [https://perma.cc/AZY7-KY9L]; *see also IoT Cybersecurity Improvement Act of 2020*, 15 U.S.C. §§ 278g-3a to 278g-3e (establishes minimum cybersecurity requirements for IoT technology procured by the U.S. government and directs federal agencies to only procure devices that comply with NIST guidelines (NIST SP 800-213 and 213A) and establishes vulnerability reporting requirements for products sold to the U.S. government).

[26] *IoT Executive Order* at 26635-26637.

[27] OMB, Memorandum for the Heads of Executive Departments and Agencies at 5, 7 (2023), https://www.whitehouse.gov/wp-content/uploads/2023/12/M-24-04-FY24-FISMA-Guidance.pdf [https://perma.cc/X3RZ-B7GQ].

[28] *IoT Labeling NPRM* at 5-6, para. 7.

[29] NIST, Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products (2022), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf [https://perma.cc/D59M-BZWD] (*NIST Cybersecurity White Paper*).

[30] NIST, NISTIR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers (2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf [https://perma.cc/RZE8-SDRZ]; NIST, NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline (2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf [https://perma.cc/C9AK-2PGA]; NIST, NISTIR 8259B, IoT Non-Technical Supporting Capability Core Baseline (2021) https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8259B.pdf [https://perma.cc/6KJK-D2NB]; *see also* NIST, *NIST Cybersecurity for IoT Program, NISTIR 8259 Series* (Nov. 16, 2021) https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series [https://perma.cc/8HKR-XDH2].

[31] NIST, NISTIR 8425, Profile of the IoT Core Baseline for Consumer IoT Products at 1 (2022), https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.pdf [https://perma.cc/X8PK-4TV7] (NISTIR 8425).

[32] NIST, *NIST IoT Cybersecurity Program Releases Two New Documents* (Sept. 20, 2022) https://csrc.nist.gov/News/2022/nist-iot-cybersecurity-program-nist-irs-8425-8431 [https://perma.cc/6748-XXXX].

[33] NISTIR 8425 at 2-5.

choices about their IoT purchases.[34] From all of these efforts, NIST has identified key elements of a labeling program that encourage innovation while remaining practical and not burdensome. Most recently, in December 2023, NIST published an *IoT Product Component Requirements Essay* discussing possible standards that may be related to the NISTIR 8425 outcomes. In the essay, NIST notes that "[c]ybersecurity of IoT devices, though critical, is incomplete if cybersecurity of other IoT product components is not considered as well since the IoT device and other IoT product components will be a system."[35] NIST also clarified that the "cybersecurity technical and non-technical outcomes defined in the NISTIR 8425 consumer profile apply to IoT *products* and not just IoT devices."[36]

9. As the Commission acknowledged in the *IoT Labeling NPRM*,[37] NIST's essential work in this arena coupled with the significant private sector contributions and innovations in developing cybersecurity certification programs, Commission experience guiding compliance assessment programs,[38] and prior Commission action in this space,[39] provide the building blocks for our development and adoption of this IoT Labeling Program. We continue to consider closely the work of NIST in support of our IoT labeling efforts.

10. The private sector has also taken measures to promote IoT security. As we noted in the *IoT Labeling NPRM*, for example, the Consumer Technology Association (CTA) has convened an IoT working group tasked with supporting the advancement of the consumer IoT industry,[40] and produced a white paper addressing the current regulatory approach to IoT.[41] The record also references additional

[34] *See id.* at 16; *see also* NIST, *Consumer Cybersecurity Labeling Pilots: The Approach and Contributions* (May 24, 2022), https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/consumer-cybersecurity-labeling-pilots [https://perma.cc/7TGC-PXVJ].

[35] NIST, Identifying Standards and Guidance for a Consumer IoT Product Development Handbook (2023), https://www.nist.gov/system/files/documents/2023/11/30/FINAL_IoT%20Product%20Requirements%20Discussion%20Essay_20231129.pdf [https://perma.cc/UG83-72FJ] (NIST IoT Product Component Requirements Essay).

[36] *Id.*

[37] *IoT Labeling NPRM* at 6, para. 8.

[38] *See, e.g.,* 47 CFR pt. 2, Subpart J (equipment authorization); 47 CFR § 20.19 (hearing aid compatibility); 47 CFR §§ 2.1091, 2.1093 (radiofrequency radiation exposure); 47 CFR pt. 68 (connection of terminal equipment to the telephone network).

[39] *See Spectrum Requirements for the Internet of Things*, ET Docket No. 21-353, Notice of Inquiry, 36 FCC Rcd 14165 (2021); *Supply Chain NOI*, 36 FCC Rcd 10578, (2021); Report and Order, Order, and Further Notice of Proposed Rulemaking, FCC 22-84 (Nov. 11, 2022); *Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band*, ET Docket No. 13-49, First Report and Order, 29 FCC Rcd 4127, 4143, para. 54 (2014).

[40] Consumer Technology Association CES, *IoT Working Group*, https://www.cta.tech/Membership/Member-Groups/IoT-Working-Group [https://perma.cc/9ULY-PJ6E] (last visited Nov. 24, 2023).

[41] ANSI/CTA, Standard Baseline Cybersecurity Standard for Devices and Device Systems ANSI/CTA-2088-A (2022), https://shop.cta.tech/products/https-cdn-cta-tech-cta-media-media-shop-standards-2020-ansi-cta-2088-a-final-pdf [https://perma.cc/8ES6-VN3B]; *see also* Consumer Technology Association, Smart Policy to Secure our Smart Future: How to Promote a Secure Internet of Things for Consumers (2021), https://shop.cta.tech/collections/research/products/smart-policy-to-secure-our-smart-future-how-to-promote-a-secure-internet-of-things-for-consumershttps://shop.cta.tech/collections/research/products/smart-policy-to-secure-our-smart-future-how-to-promote-a-secure-internet-of-things-for-consumers [https://perma.cc/BRM2-CR5A] (CTA Cybersecurity White Paper); *Supply Chain NOI*, 36 FCC Rcd 10578, para. 104 (seeking comment on the CTA Cybersecurity White Paper). CTA has also convened with various organizations to discuss IoT baseline security capabilities. *See* Council to Secure the Digital Economy, The C2 Consensus on IoT Device Security Baseline Capabilities (2019), https://csde.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf [https://perma.cc/2GVK-GFM6]; Council to Secure the Digital Economy, The C2 Consensus on IoT Device Security Baseline Capabilities – 2021 Supplement (2021), https://csde.org/wp-content/uploads/2021/04/C2-Tech-Report_2021_final.pdf [https://perma.cc/U45C-DGYT]; *IoT Labeling NPRM* at 4, para. 5.

efforts undertaken by our industry partners to address IoT vulnerabilities. For example, Comcast notes how their "Comcast Xfinity PKI system (xPKI) provides individual identity to millions of IoT devices on a daily basis through secure automation and standards compliance."[42] Samsung highlights that, in order to function with their "SmartThings platform and receive the 'Works with SmartThings' certification, all devices must pass (1) functional testing for seamless interoperability and (2) security testing for secure connections."[43] It is against these multiple efforts as a backdrop that we take action today to leverage, unify, and elevate efforts to date within a common programmatic framework.

III. REPORT AND ORDER

A. Voluntary IoT Labeling Program

11. Today, we establish a voluntary IoT Labeling Program for wireless consumer IoT products. While participation is voluntary, those that choose to participate must comply with the requirements of the IoT Labeling Program to receive authority to utilize the FCC IoT Label bearing the Cyber Trust Mark. The *IoT Labeling NPRM* sought comment on whether the proposed IoT Labeling Program should be voluntary,[44] reasoning that "success of a cybersecurity labeling program will be dependent upon a willing, close partnership and collaboration between the federal government, industry, and other stakeholders."[45] The record shows substantial support for a voluntary approach.[46] CEDIA suggests that IoT Labeling Program must be voluntary "for the program to gain momentum in the marketplace."[47] AIM, Inc. suggests that the voluntary aspect of the IoT Labeling Program "will help drive adoption of the label by device producers."[48] Further, commenters suggest that a voluntary program will ensure the broadest reach, most efficiency, and widest access to a diversity of IoT technologies.[49] We agree that a voluntary program will help drive adoption of the IoT Labeling Program, so that a willing, close partnership can be achieved. We also agree with the record that flexible, voluntary, risk-based best practices are the hallmarks of IoT security as it exists today and as it is being developed around the world.[50] Additionally, we acknowledge the view that "consumer labeling is a difficult undertaking in any context,"[51] especially in the evolving area of cybersecurity, and that the "best approach is to start the Program with something achievable and effective."[52] We concur that willing participation will allow the IoT Labeling Program to be more easily achievable than requiring participation in a novel program. With the added imprimatur of a U.S. government certification mark, the IoT Labeling Program will help

[42] Comcast Comments at 4.

[43] Samsung Comments at 2.

[44] *IoT Labeling NPRM* at 6, para. 9.

[45] *Id.*

[46] USTelecom at 2; CTIA Comments at 15; NCTA Comments at 4; Samsung Electronics America Comments at 5 (Samsung); Comcast Comments at 1*; see also* Open Voice Network Comments at 4 (OVON); Alliance for Automotive Innovation Comments at 2 (Auto Innovators; Plumbing Manufacturers International Comments at 2 (PMI); Custom Electronic Design & Installation Association Reply at 3 (CEDIA); Infineon Technologies Americas Corp. Reply at 2-3 (Infineon); EPIC Reply at 4.

[47] CEDIA Reply at 3.

[48] AIM, Inc. Comments at 3 (AIM).

[49] Consumer Technology Association Reply at 3 (CTA) (citing Association of Home Manufacturers Comments at 2 (AHAM)); Consumer Technology Association Comments at 4 (CTA); CTIA – The Wireless Association Comments at 15 (CTIA); National Association of Manufacturers Comments at 2 (NAM); NTCA Comments at 4; Telecommunications Industry Association Comments at 2 (TIA); USTelecom – The Broadband Association Comments at 11-12 (USTelecom); Widelity Comments at 1-4; Wi-Fi Alliance Comments at 10.

[50] CTIA Comments at 15.

[51] CTIA Reply at 1.

[52] Infineon Reply at 2.

distinguish products in the marketplace that meet minimum requirements and provide options to consumers.

12. We reject arguments that mandating participation in the IoT Labeling Program is necessary.[53] While we recognize that a voluntary IoT Labeling Program may cause concern that smaller businesses with limited resources may choose not to participate,[54] we believe the strong stakeholder engagement and collaboration that we expect to result from willing participation, and which is vital to establishing this new program, outweighs these risks. Further, while we acknowledge that, at least in the near term, allowing the IoT Labeling Program to be voluntary "could limit its adoption and impact,"[55] we believe this risk is outweighed by the benefits that a voluntary program will garner, such as speed to market to hasten impact, efficiency of resources, and the likelihood that consumer demand will drive widespread adoption over time.

13. In adopting the IoT Labeling Program with the parameters discussed in this Order, we are establishing a collaborative effort between the federal government and relevant stakeholders in industry and the private sector. We emphasize that this Order is intended to provide the high-level programmatic structure that is reasonably necessary to establish the IoT Labeling Program and create the requirements necessary for oversight by the Commission, while leveraging the extensive work, labeling schemes, processes and relationships that have already been developed in the private sector. We also note that there is further development to be done by the private sector and other federal agencies to implement the IoT Labeling Program and, as discussed below, expects many of the details not expressly addressed in this Order will be resolved through these separate efforts and by the authorities the Commission delegates to the Public Safety and Homeland Security Bureau (PSHSB or the Bureau).

B. Eligible Devices or Products

14. As explained herein, today's Order initially establishes the IoT Labeling Program for wireless consumer IoT products. We do not, however, foreclose the possibility of expanding the IoT Labeling Program in the future. In the *IoT Labeling NPRM*, we sought comment on the scope of devices or products for sale in the United States that should be eligible for inclusion in the IoT Labeling Program, asking what would provide the most value to consumers.[56] We sought comment on whether the IoT Labeling Program should include IoT "devices" or "products," [57] and proposed that those eligible should include intentional radiators that generate and emit radio frequency (RF) energy by radiation or induction.[58] Additionally, the *IoT Labeling NPRM* sought comment on whether to focus on consumer IoT or to include enterprise IoT.[59]

15. As described below, the record supports adopting the IoT Labeling Program that encompasses consumer-focused IoT products. We focus our IoT Labeling Program initially on consumer IoT products, rather than enterprise or industrial IoT products. Because medical devices regulated by the U.S. Food and Drug Administration (FDA) already are subject to statutory and regulatory cybersecurity requirements under other federal laws more specifically focused on such devices, we do not include such devices in our IoT Labeling Program. We also exclude from our IoT Labeling program any communications equipment on the Covered List that the Commission maintains pursuant to the Secure

[53] Paul Cabral Comments at 1; Bryce Gilchrist Comments at 1; Kenneth Johnson Comments at 1; *see also* Internet Safety Labs Comments at 2 (recommending that the IoT Labeling Program become mandatory over time).

[54] *See* Michael Ravnitzky Comments at 1 (Ravnitzky).

[55] *Id*.

[56] *IoT Labeling NPRM* at 6, para. 10.

[57] *Id.* at 8, para. 13.

[58] *Id.* at 7, para. 12.

[59] *Id.* at 8, para. 16.

and Trusted Communications Networks Act and equipment produced by certain other entities as discussed below. Finally, our initial IoT Labeling Program will focus on wireless consumer IoT devices consistent with the core of our section 302 authority governing the interference potential of devices that emit radio frequency energy—and thus we exclude wired IoT devices at this time.

16. *Definition of IoT Devices*. Although we focus our IoT Labeling program on IoT "products," to lay a foundation we must first address the definition of IoT "devices" because this definition is a building block of the IoT "product" definition. In this respect, we adopt the modified version of the NIST definition of "IoT device" that the Commission proposed in the *IoT Labeling NPRM*.[60] Specifically, the *IoT Labeling NPRM* proposed defining an IoT device to include (1) an Internet-connected device capable of intentionally emitting RF energy that has at least one transducer (sensor or actuator) for interacting directly with the physical world, coupled with (2) at least one network interface (e.g., Wi-Fi, Bluetooth) for interfacing with the digital world.[61] This definition builds on NIST's definition by adding "Internet-connected" as a requirement, because "a key component of IoT is the usage of standard Internet protocols for functionality."[62] The modified definition adopted today also adds that a device must be "capable of intentionally emitting RF energy," because aspects of the Commission's authority recognizes the particular risks of harmful interference associated with such devices.[63]

17. The record supports this reasoning. For example, Consumer Reports states that "[i]f you're going to sell a device where some of the benefits come from having a cloud connection, an app, and connectivity, then those must also be secured."[64] Consumer Reports provides further support for the Commission's reasoning by noting that "connectivity may be so central to the functionality of the device that it may no longer be able to operate safely [without it]."[65] TIC Council Americas similarly "agrees that 'internet-connected' should be included in the definition of IoT devices."[66] We agree with these arguments and adopt the modified IoT device definition requiring "Internet-connected" device element to assure consumers that the functionality of the IoT device or product displaying the Cyber Trust Mark is reasonably secure as well. As noted by ioXt Alliance, including "Internet-connected" in the definition of IoT makes "sense if the program focuses on IoT products instead of devices because not all IoT devices are 'internet-connected.'"[67] Because the IoT Labeling Program will be focused on the broader category of IoT consumer products and not devices, including "Internet-connected" in the definition of IoT device is further justified.

18. We disagree with commenters who argue the Commission should adopt the NIST definition of a device without change.[68] We acknowledge that the record indicates some concern regarding the Internet-connected element of the Commission's proposed definition; however, we find these concerns to be misplaced. TIC Council Americas, for example, supports adding "Internet-

[60] *Id.* at 7, para. 11.

[61] *Id.*

[62] *Id*. (citing NISTIR 8425 at 23).

[63] 47 U.S.C. § 302a; *see also* FCC, *Equipment Authorization, Marketing, and Importation (Including Jammers)* (Dec. 20, 2022), https://www.fcc.gov/enforcement/areas/equipment-authorization-marketing-importation#:~:text=47%20U.S.C.,harmful%20interference%20to%20radio%20communications [https://perma.cc/YL8M-WMAH]. ("The Commission adopted rules to ensure that radio frequency devices comply with the Commission's technical standards, as well as labeling and information disclosure requirements, to prevent harmful interference from occurring once devices are sold to the public.").

[64] Consumer Reports Comments at 6.

[65] *Id.* at 26.

[66] TIC Council Americas Comments at 3.

[67] ioXt Alliance Comments at 7-8.

[68] Connectivity Standards Alliance Comments at 3 (CSA); AIM Comments at 2.

connected" to the definition, but argues that "there are devices that are able to connect to non-internet connected networks, and that those devices should not be excluded from the program."[69] While we do not foreclose the possibility of expanding the IoT Labeling Program to devices on non-internet connected networks in the future, we focus initially on the more common category of Internet-connected consumer IoT products. Others argue that "Internet-connected" is too "situational,"[70] with a concern that the device might become "disconnected from the internet and, therefore, no longer be an 'IoT device.'"[71] We do not agree that "Internet-connected device" must be interpreted so narrowly as to exclude from the IoT Labeling Program devices that may become disconnected from the Internet. "Internet-connected," in terms of the IoT Labeling Program, applies to the functional capability of the device; if the device is capable of being connected to the Internet, the fact that it may not be connected at any given point in time does not exclude its eligibility for participation in the IoT Labeling Program. Further, any potential concerns arising from requiring an IoT device be "Internet-connected" for inclusion in the IoT Labeling Program are outweighed by the benefit of giving consumers further assurance that the security of their IoT device or product extends to the connected functionality that a consumer expects when making such a purchase. In this respect, including "Internet-connected" in the definition of IoT device also recognizes the highest risk functional component of an IoT device that distinguishes "smart" devices from other devices a consumer may use, and allows the Cyber Trust Mark to more effectively support consumer expectations.

19. The record also supports adding an RF energy-emitting element to the IoT device definition, acknowledging the Commission's authority under Section 302 governing the interference potential of devices that emit RF energy and can cause harmful interference to radio communications.[72] We reject the argument that limiting the definition to RF-emitting devices may lead to marketplace confusion if a product does not bear the Cyber Trust Mark due solely to its lack of RF energy emissions.[73] In the first instance, we note the need to launch an achievable IoT Labeling Program consistent with the Commission's core authority. We also note that the benefits that a focus on wireless products will have in elevating the overall cybersecurity posture of the IoT ecosystem, especially in view of the record indicating that the majority of IoT devices are wireless,[74] outweigh the risks associated with concerns regarding marketplace confusion. In any case, there will be a number of products – both wired and wireless – that do not bear the Cyber Trust Mark while uptake occurs. We also anticipate that consumer education in this space will help alleviate these concerns.

20. We further disagree with the view that the capability of a device to emit RF radiation is "unrelated to the general, far-ranging cybersecurity concerns the Commission is confronting in this proceeding."[75] Instead, we agree with Comcast that interference caused by a [distributed denial of service] attack raises "the same policy concerns and has the same practical effect as interference caused

[69] TIC Council Americas Comments at 3.

[70] CSA Comments at 2.

[71] *Id*.

[72] Comcast Comments at 13 ("Specifically, the text and history of Section 302 strongly support the arguments set forth in the NPRM that the Commission has the authority to move forward with the program."); CTA Comments at 8 ("Therefore, the Commission's proposal to establish rules … for this voluntary labeling program fall within the scope of the FCC's Section 302 authorities.").

[73] CSA Comments at 3; *see also* AIM Comments at 2 (noting potential confusion from limiting the NIST definition). We also note that for now, we are limiting the class of devices eligible for the Cyber Trust Mark to wireless intentional radiators, as discussed in para. 37, *infra*.

[74] Consumer Reports Reply at 3 (explaining that "wireless devices are the majority of IoT devices.").

[75] USTelecom Comments at 13; *see also* CTIA Reply at 4 ("Attacks that seek to weaponize radiofrequency interference, while theoretically possible, are not a major risk.").

by traditional means."[76] EPIC explains how hackers exploit unpatched vulnerabilities to attack a large number of wireless devices, and turning them into signal jammers to take down mobile networks.[77] The record thus bears out our view that cybersecurity vulnerabilities in wireless IoT devices could cause harmful interference to radio communications. Given Congress' direction to the Commission in Section 302 of the Act to guard against the interference potential of wireless devices, requiring the element of "emitting RF energy interference" in the IoT device definition for the initial iteration of the IoT Labeling Program focuses on that core Commission authority without ruling out future action regarding wired IoT devices.[78] Further, while we acknowledge that devices that unintentionally or incidentally emit RF radiation may also pose interference potential, we find that a focus initially on "intentional" radiators provides the ability of a nascent program to target products with the highest risk profile from among those that emit RF energy.

21. *Definition of IoT Products*. We adopt the NIST definition of an "IoT product."[79] Specifically, the *IoT Labeling NPRM*'s proposed definition of IoT product is an "IoT device and any additional product components (e.g., backend, gateway, mobile app) that are necessary to use the IoT device beyond basic operational features."[80] The record supports adopting the IoT product definition developed by NIST, with Garmin International, Inc. (Garmin) noting that a fundamental purpose of the IoT Labeling Program "is to inform consumers regarding device security as they evaluate potential IoT purchases. . . . [T]his purpose is best achieved by focusing on 'consumer IoT products' as defined by NIST in NISTIR 8425." [81] Additionally, Kaiser Permanente states that adopting the NIST definition of IoT products will "promote consistency across federal agency programs and related industry norms and requirements."[82] Further, the Information Technology Industry Council (ITI) explained that the "Commission's implementation of the program will be more successful if it aligns as closely as possible to the definitions, processes and procedures already outlined by NIST."[83] We agree with these commenters, in that adopting NIST's IoT product definition will allow for consistency in the treatment of programmatic elements across the federal government, and allow the Commission to appropriately leverage the work existing in this space to promote the IoT Labeling Program's success. We also note that no commenters opposed the NIST definition of IoT products. For purposes of the IoT Labeling Program, when discussing IoT products and their "components" in this Report and Order, we are using the NISTIR 8425 scoping definition of "components." We believe that this definition allows the IoT Labeling Program to address the most relevant "package" components expected by consumers to be securable when making purchasing decisions, and encompasses the appropriate level of "component" pieces to address the functionalities that generate the most salient cybersecurity risks.[84] This view is

[76] Comcast Comments at 15.

[77] EPIC Reply at 5.

[78] We discuss further below our initial focus of the IoT Labeling Program on wireless devices. *See infra* paras. 37-39.

[79] *IoT Labeling NPRM* at 8, para. 13.

[80] *Id.*

[81] Garmin International, Inc. Comments at 6 (Garmin); *see also* Everything Set, Inc. Comments at 3 ("We believe the cybersecurity labeling program should be focused on IoT products consistent with the NIST definition.").

[82] Kaiser Permanente Comments at 2.

[83] Information Technology Industry Council Comments at 4 (ITI).

[84] For purposes of the IoT Labeling Program, the NISTIR 8425 scoping definition of "components" falls into three main types: Specialty networking/gateway hardware (e.g., a hub within the system where the IoT device is used); Companion application software (e.g., a mobile app for communicating with the IoT device); and Backends (e.g., a cloud service, or multiple services, that may store and/or process data from the IoT device). *See* NISTIR 8425 at 2. Our use of this scoping definition of "components" is intended only to apply to the IoT Labeling program. We note

(continued….)

supported by the record, with CTA providing a proposed testing framework where "all individual components provided by the manufacturer should be in scope for testing," including all components of the IoT product "that are necessary for the device to function in a normal use case scenario."[85]

22. *IoT Devices vs. IoT Products*. We find that the IoT Labeling Program should apply to "IoT products" as defined above, rather than being limited only to "IoT devices." In the *IoT Labeling NPRM*, the Commission noted that it was important to ensure that the IoT Labeling Program "would be sufficiently inclusive to be of value to consumers."[86] Since the Commission's adoption of the *IoT Labeling NPRM*, NIST has provided clarity in this realm by stating "the cybersecurity technical and non-technical outcomes defined in the NISTIR 8425 consumer profile apply to IoT products and not just IoT devices."[87] In addition, in reviewing the record, we believe applying the IoT Labeling Program to IoT products instead of IoT devices alone achieves these priorities because only by addressing the full functionality of a consumer product (i.e., one or more IoT devices and any additional product components (e.g., backend, gateway, mobile app) that are necessary to use the IoT device, beyond basic operational features) will provide consumers the necessary scope to satisfy the basic security expectation of the consumer and effectuate a discernable increase in the cybersecurity posture of the IoT ecosystem at large.

23. There is significant support in the record for an IoT product focus for the IoT Labeling Program.[88] As explained by UL Solutions, applying the IoT Labeling Program to IoT products is necessary since "most IoT devices sold to consumers cannot be meaningfully used without additional components."[89] The Cybersecurity Coalition further supports this position by saying "IoT devices are typically part of a broader ecosystem of components that can have their own security issues, requiring 'IoT cybersecurity' to extend beyond individual devices to be effective."[90] ITI notes an IoT product focus benefits consumers because it "will appropriately capture the relevant devices/components of the product that could be vulnerable to attack (and are always included in an IoT product, as NIST points out)."[91] Applying the IoT Labeling Program to IoT products further benefits consumers by promoting consumer safety because it "encourages manufacturers to prioritize security across all components, ultimately leading to safer and more reliable IoT experiences for consumers."[92] Additionally, the record indicates that "the entire service which includes cloud infrastructure as well as apps or other ways to control or manage the device by the user, and not simply the physical device itself, is critical for an assessment of safety and security."[93] Further, focusing on IoT products aligns not only with the technical requirements of NISTIR 8425, but also "emerging requirements in Europe and the UK, such as the EU [Cyber

that Commission rules use the term "components" in a variety or contexts and different rule provisions, and we are not intending to affect the use of that term in those other contexts.

[85] Letter from J. David Grossman, Vice President, Regulatory Affairs, CTA, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 23-239, at 9 (filed Feb. 8, 2024) (CTA *Ex Parte*).

[86] *IoT Labeling NPRM* at 6, para. 10.

[87] NIST IoT Product Component Requirements Essay at 1.

[88] *See, e.g.*, Cybersecurity Coalition Comments at 3; UL Solutions Comments at 2; IEEE 802 LAN/MAN Standards Committee at 3; ITI Comments at 2; International Speech and Communication Association Special Interest Group: Security and Privacy in Speech Communication Comments at 2 (ISCA); Consumer Reports Comments at 6 ("The definition of an IoT device must include all elements of an IoT system."); Connected Consumer Device Security Council (CCDS) Comments at 1-2.

[89] UL Solutions Comments at 2.

[90] Cybersecurity Coalition Comments at 3.

[91] ITI Comments at 3.

[92] ISCA Comments at 2.

[93] Everything Set, Inc. Comments at 3.

Resilience Act], and EU Directives on consumer protections EU 2019/770, 771."[94] We agree and will apply the IoT Labeling Program to consumer IoT products, which provides for the greatest level of consumer benefit by prioritizing cybersecurity across the entirety of the consumer product, as compared to just the device, which is able to perform its full functionality only when working in conjunction with other product components.

24. We disagree with Samsung, CTIA, LG Electronics, and CTA, who advocate focusing on IoT devices instead of IoT products.[95] Samsung and CTIA argue that cybersecurity standards for devices are more mature than standards for products,[96] and CTA argues that applying the FCC IoT Label to products would be more complex than devices.[97] LG Electronics expresses concern that expanding to products "would require device manufacturers to attest to the security of product components that are outside of their control."[98] We do not agree that these rationales support limiting application of the IoT Labeling Program only to devices, rather than products. First, applying the IoT Labeling Program narrowly to IoT devices would run counter to NIST's guidance and considerable work in this space, upon which the Commission has relied for the basis for the IoT Labeling Program proposal. NIST's *Profile of the IoT Core Baseline for Consumer IoT Products* (NISTIR 8425), discussed above, provides fundamental IoT guidelines and applies to the broader product category,[99] and the more recent *NIST IoT Product Component Requirements Essay* clearly states that the outcomes listed in NISTIR 8425 apply to consumer IoT products and not just IoT devices.[100]

25. Further, regarding the notion that the IoT Labeling Program should be focused on IoT devices because existing standards for IoT devices are more readily available or achievable in the near term, we counter that the record shows existing IoT device standards can be leveraged to support assessing IoT products as well. As noted by commenter ITI, existing IoT industry standards "capture similar baseline themes" to the NIST criteria.[101] In view of these similarities, the IoT Labeling Program can leverage these existing standards for IoT devices as building blocks, and tailor them in view of the IoT products being assessed. Accordingly, the need to realize the benefits of a product-level label weigh in favor of taking a small amount of time to get to product-based standards by leveraging existing device standards.

26. We also reject the argument that because "cybersecurity frameworks and testing programs have been developed to focus on device-level—rather than product-level—assessment" that a device-level IoT Labeling Program is the appropriate outcome.[102] We note, for example, that ITI recommends recognizing IoT security assessments from our international partners, such as IoT

[94] Letter from Dr. Amit Elazari, CEO and Co-Founder, OpenPolicy, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 23-239, at 4 (filed Jan. 24, 2024).

[95] Samsung Comments at 4; CTIA Comments at 21; LG Electronics USA Inc. Comments at 1 (LG Electronics); CTA Comments at 14.

[96] *See, e.g.*, Samsung Comments at 4 ("However, given the relative maturity of IoT device cybersecurity criteria and standards, the Commission should focus the scope of the Program initially on IoT devices…."); *see also* CTIA Comments at 21 ("Because many frameworks and resources in the market, including the NISTIR 8259 series upon which the Commission seeks to build the program, are focused on device-level criteria, widening the scope of the program to encompass the entire IoT "product" would create significant complications….").

[97] CTA Comments at 14.

[98] LG Electronics Comments at 1.

[99] *See generally* NISTIR 8425.

[100] NIST IoT Product Component Requirements Essay at 1.

[101] ITI Comments at 6.

[102] Letter from David Valdez, Vice President, Privacy & Cybersecurity Policy, CTIA, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 23-239, at 4 (filed Jan. 8, 2024) (CTIA *Ex Parte*).

assessments under the Cybersecurity Labelling Scheme (CLS) by Singapore's Cyber Security Agency, which assesses the overall IoT product, and not just a single device included in the IoT product.[103] In this regard, the ability to recognize international efficiencies for IoT Labeling Program participants would be hindered by limiting the Cyber Trust Mark to the device level, as Singapore's CLS (and other evolving international standards) focus on product-level assessments.

27. Finally, applying the IoT Labeling Program to products enhances value to consumers without requiring manufacturers to be responsible for products or devices that are outside of their control. The record shows that a consumer's expectation of security extends to the entire IoT product they purchase. This consumer expectation is evidenced in the record by ITI, clarifying that "because consumers purchase, interact with, and view IoT merchandise not as component parts but as complete physical product . . . Consumers are primarily concerned with the entire physical product they are purchasing."[104] Additionally, as noted by UL Solutions, "most IoT devices sold to consumers cannot be meaningfully used without additional components."[105] In view of this need, a manufacturer seeking authority to affix the FCC IoT Label is expected to secure the whole IoT product, including the product's internal communication links connecting the different parts of the product to each other as well as the product's communication links that connect the IoT product to the outside world. We do not require manufacturers to be responsible for third-party products or devices (including apps) that are outside of their control; however, where a manufacturer allows third-party apps, for example, to connect to and control their IoT product such manufacturer is responsible for the security of that connection link and the app if such app resides on the IoT product. Moreover, NIST enumerates the dangers of an IoT device-only focus, establishing that the "additional product components have access to the IoT device and the data it creates and uses-making them potential attack vectors that could impact the IoT device, customer, and others,"[106] and that "these additional components can introduce new or unique risks to the IoT product."[107] Consumer expectations that the FCC IoT Label would apply to the entirety of the product purchased is further highlighted by Consumer Reports, explaining that "If everything is sold within a box, then everything in the box should be approved to use the mark."[108] Consumer Reports also notes that "[i]f the labeling programs were only to address the physical device and not other system components, consumers would likely be deceived as to the scope and efficacy of the program."[109] The record is adamant that the "Cyber Trust Mark must be trusted by consumers to be successful."[110] In view of the record, securing only a portion of an IoT product by just assessing a single IoT device included in the IoT product, instead of assessing the devices and components that comprise the IoT product holistically, could deceive consumers and go against consumer expectation that the technology being brought into their homes is reasonably secure. We weigh heavily the likelihood for consumer confusion should the device-only approach be taken, and accordingly we apply this consumer IoT Labeling Program to IoT products and not just IoT devices.

[103] ITI Comments at 6; Singapore Cyber Security Agency, Cybersecurity Labelling Scheme for IoT Publication No. 2 at 10 (Sept. 2023), https://www.csa.gov.sg/docs/default-source/our-programmes/certification-and-labelling-scheme/cls/publications/-pub-ccc-sp-151-2-cls(iot)-scheme-specifications-v1.3.pdf?sfvrsn=5c9ace5f_1 [https://perma.cc/3C2J-QWXE] (requiring the testing lab to "determine if the firmware *and companion mobile application* of the Device Under Test (DUT) is free from common software errors such as buffer overflown [sic], known vulnerabilities in any of the third-party libraries being used, and known malware." [emphasis added]).

[104] ITI Comments at 4.

[105] UL Solutions Comments at 2.

[106] NISTIR 8425 at 3.

[107] *Id.*

[108] Consumer Reports Comments at 6.

[109] *Id.*

[110] Whirlpool Corporation Comments at 6 (Whirlpool).

28. In sum, although there are relative advantages and disadvantages with either a narrow focus on IoT devices or a broader focus on IoT products, on balance we are persuaded to focus our initial IoT Labeling Program on IoT products. As explained above, we find commenters' concerns about encompassing full IoT products in our IoT Labeling Program to be overstated. At the same time, we see significant shortcomings with a narrower focus just on IoT devices. Weighing the totality of these considerations, we are persuaded that targeting the IoT Labeling Program on IoT products is the best approach at this time.

29. *Consumer IoT Products vs. Enterprise IoT Products*. The *IoT Labeling NPRM* sought comment on whether we should focus the IoT Labeling Program on IoT products intended for consumer use or include products intended for industrial or business use.[111] Specifically, the *IoT Labeling NPRM* noted that "IoT devices and products have proliferated not only in the non-enterprise space, but also in the workplace from office settings to field settings, from medical settings to industrial settings."[112] The IoT Labeling Program we adopt today applies to the labeling of consumer IoT products that are intended for consumer use,[113] and does not include products that are primarily intended to be used in manufacturing, healthcare, industrial control, or other enterprise applications. While we do not foreclose expansion of the IoT Labeling Program at a later date, this initial scope will provide value to consumers most efficiently and expediently, without added complexity from the enterprise environment.

30. The record supports the IoT Labeling Program having a consumer IoT focus, with support provided by UL Solutions, the Cybersecurity Coalition, and the Connectivity Standards Alliance, among others.[114] The FDA also suggests that IoT outside of the consumer scope may need "[g]reater and more tailored controls," suggesting that different considerations might attend IoT with a purpose outside of that in the routine consumer realm.[115] Additionally, commenters highlight the differing security needs of consumer and enterprise products.[116] For example, UL Solutions notes that "IoT products intended for commercial or industrial settings are exposed to different types of threats than consumer products and often carry higher risk if breach, which necessitates different requirements."[117] CSA also highlights that "[e]nterprise device security approaches are often customized and vary based on the specific needs of the business."[118] We agree that applying the IoT Labeling Program to consumer IoT products will reduce complexity, which will bolster the likelihood of success when starting the new IoT Labeling Program.

31. ISCA supports including enterprise IoT, stating that a broader scope will ensure the IoT

[111] *IoT Labeling NPRM* at 8, para. 16.

[112] *Id.*

[113] Some of the IoT devices and products that are intended for consumer use include smart thermostats, smart lights, smart locks, smart cameras, smart watches and fitness trackers. *See* Philips Healthcare Comments at 2 (listing smart doorbells and smart thermostats as examples of consumer IoT products).

[114] UL Solutions Comments at 2; Cybersecurity Coalition Comments at 4 ("The Commission should leverage [the] existing work on consumer IoT and not delay implementation of a consumer-focused label by attempting to cover non-consumer products as well . . . ."); CSA Comments at iii; Consumer Reports Comments at 9 ("[B]idirectional communications devices that interact with an enterprise, medical, or utility network" should be outside the scope of the IoT Labeling Program.); *see also* ioXt Alliance Reply at 4; IEEE 802 LAN/MAN Standards Committee Comments at 3; Medical Imaging & Technology Alliance Comments at 2; National Electronic Manufacturers Association Comments at 5 (NEMA); Garmin Comments at 9; TIC Council Americas Comments at 3; ITI Comments at 2. *But see* Kaiser Permanente Comments at 2-3 (arguing the Commission should include devices and products used by consumers, corporations and organizations across all industries, but exclude devices and products identified to pose an unacceptable risk to national security).

[115] Center for Devices and Radiological Health, U.S. Food and Drug Administration Comments at 5 (FDA).

[116] *See, e.g.*, UL Solutions Comments at 2; CSA Comments at 5.

[117] UL Solutions Comments at 2.

[118] CSA Comments at 5.

Labeling Program remains flexible to the extent that the boundary between consumer and enterprise IoT is blurring.[119] Further, ISCA and Abhishek Bhattacharyya note that attackers have more to gain from targeting enterprise settings.[120] While there are considerable threat vectors and vulnerabilities associated with all classes of IoT products,[121] we agree with Everything Set, Inc., that focusing the IoT Labeling Program on household use of IoT products will be more useful and have greater impact, given that enterprises tend to have more time, resources, and expertise to devote to network security.[122] They note further that many small- and medium-sized businesses also buy consumer devices, so a consumer-focused Cyber Trust Mark would be of utility to them, as well.[123] We believe in the near term that a consumer focus will provide the most initial impact, and create a level of recognition and trust in the Cyber Trust Mark itself as the IoT Labeling Program progresses that could be leveraged to enterprise IoT at a later time, and we therefore defer consideration of the IoT Labeling Program's expansion.

32. *Exclusion of Medical Devices/Products.* As an initial matter, we exclude from the IoT Labeling Program medical devices regulated by the U.S. Food and Drug Administration (FDA).[124] The Center for Devices and Radiological Health (within the FDA) expresses concern that the Commission's labeling IoT Labeling Program may lack controls and minimum criteria that it believes are necessary for IoT medical devices.[125] In addition, the FDA is concerned that including medical devices in the IoT Labeling Program may cause consumer confusion and "potentially creates conflict where product manufacturers attempt to both qualify for the Cyber Trust Mark and comply with existing statutory and regulatory cybersecurity requirements under other federal laws, such as the Federal Food, Drug, and Cosmetic Act (FD&C Act)."[126] These considerations persuade us to exclude FDA-regulated medical devices from our IoT Labeling Program, consistent with commenters' recommendations.

33. *Exclusion of Devices/Products Produced by Certain Entities.* We adopt the following measures to promote national security in connection with the IoT Labeling Program. The *IoT Labeling NPRM* proposed to exclude from the IoT Labeling Program (1) any communications equipment on the

[119] ISCA Comments at 2.

[120] *Id.*; Abhishek Bhattacharyya Comments at 1.

[121] There are many types IoT devices and products, which may be divided into various categories or classes based on their purpose, application, and functionality. These classes of IoT devices and products include smart home (e.g., smart thermostats, smart lights, smart locks, smart cameras), wearables (e.g., fitness trackers, smart watches), and Healthcare (e.g., remote patient monitoring devices, smart medical equipment). It is worth noting that not all IoT devices or products are created equal, in terms of features, security and the level of risk they present. Additionally, from security standpoint, an IoT product that is appropriate for consumer or home use may not be suitable for industrial or enterprise environment. These differences suggest the need for different security standards that distinguish between low risk, medium risk and high risk applications. Our approach to identifying the specific cybersecurity standards to apply enables us to appropriately account for that in the case of particular wireless consumer products (or categories of such products) in our initial implementation of the IoT Labeling Program.

[122] Everything Set, Inc. Comments at 3.

[123] *Id.*

[124] *See*, *e.g.*, FDA Comments at 1; Consumer Reports Comments at 15 (arguing the Commission's labeling program should not supersede the Consolidated Appropriations Act of 2023, which includes cybersecurity rules covering medical devices, including connected consumer devices such as thermometers or CPAP machines); Kevin Fu Comments at 1 (recommending the program explicitly exclude FDA-regulated medical devices from its scope "to prevent a weakening of the more rigorous FDA expectations of cybersecurity engineering"); Phillips Healthcare Comments at 2 (stating FDA requirements often go beyond what would be required in the proposed FCC program and that including medical devices in this labeling program would create confusion among users by providing an incorrect signal that an FDA-cleared medical device without the Cyber Trust Mark does not maintain high cybersecurity standards); NTCA Reply at 4.

[125] FDA Comments at 1.

[126] *Id.*

Covered List maintained by the Commission pursuant to section 2 of the Secure and Trusted Communications Networks Act (STCNA);[127] (2) any IoT device produced by an entity identified on the Covered List (i.e., an entity named or any of its subsidiaries or affiliates) as producing "covered" equipment; and (3) any device or product from a company named on certain other lists maintained by other federal agencies that represent the findings of a national security review.[128] We now adopt all of these prohibitions as they relate to our decision to focus the IoT Labeling Program on consumer IoT products. Thus, any communications equipment identified on the Covered List, now or in the future, will be ineligible for the IoT Labeling Program, and any such product will be denied approval to use the Cyber Trust Mark. Furthermore, any additional products produced by an entity identified on the Covered List as producing "covered" equipment, or any product containing devices or product components produced by such an entity, will be ineligible for the IoT Labeling Program; this would include products that may not fit within the definition of "communications equipment" under STCNA.[129] Only entities identified on the Covered List as producers of "covered" equipment—not those on the Covered List only because of their "covered" services—are subject to this prohibition.[130] In addition, we adopt the proposal that IoT devices or products containing devices manufactured by companies named on the Department of Commerce's Entity List,[131] named on the Department of Defense's List of Chinese Military Companies,[132] or suspended or debarred from receiving federal procurements or financial awards, including those published as ineligible for award on the General Service Administration's System for Award Management,[133] will not be authorized to display the FCC IoT Label or participate in the IoT Labeling Program. Further, we exclude from the IoT Labeling Program any products containing devices produced or manufactured by these entities. We conclude that inclusion on these lists represents a determination by

[127] The Secure and Trusted Communications Networks Act of 2019 requires the Commission to publish a list of "covered" communications equipment that, among others, "poses an unacceptable risk to the national security of the United States or the security and safety of United States persons." Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158, § 1603(b)(1) (2020) (codified as amended at 47 U.S.C. §§ 1601–1609). As of March 14, 2024, the Covered List includes telecommunications and video surveillance equipment produced by Huawei Technologies Company, ZTE Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, and by any of these entities' subsidiaries or affiliates. *See* FCC, *List of Equipment and Services Covered By Section 2 of The Secure Networks Act* (Oct. 6, 2023), https://www.fcc.gov/supplychain/coveredlist [https://perma.cc/7EJ4-SDCE].

[128] *IoT Labeling NPRM* at 9, para. 18.

[129] *See* 47 U.S.C. § 1608(4); 47 CFR § 1.50001(c).

[130] As of March 14, 2024, this includes Huawei Technologies Company, ZTE Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, and their subsidiaries and affiliates. *See* FCC, *List of Equipment and Services Covered By Section 2 of The Secure Networks Act* (Oct. 6, 2023), https://www.fcc.gov/supplychain/coveredlist [https://perma.cc/7EJ4-SDCE].

[131] *See* Bureau of Industry and Security, U.S. Department of Commerce, Supplement No. 4 to Part 744 – Entity List (2023), https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file [https://perma.cc/STW5-B8GW]; *see also* CTIA Comments at 39-40; Cybersecurity Coalition Comments at 4; USTelecom Comments at 2 (recommending excluding entities that appear on this list from the labeling program).

[132] *See* U.S. Department of Defense, Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. ("Mac") Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283), Tranche 2 (2022), https://media.defense.gov/2022/Oct/05/2003091659/-1/-1/0/1260H%20COMPANIES.PDF [https://perma.cc/5LMA-LZLG]; *see also* CTIA Comments at 39-40, Cybersecurity Coalition Comments at 4, and USTelecom Comments at 2 (recommending excluding entities that appear on this list from the labeling program).

[133] *See* U.S. General Services Administration System for Award Management, *Exclusion Types*, https://sam.gov/content/entity-information/resources/exclusion-types [https://perma.cc/5L45-LKCJ] (last visited Feb. 15, 2024); *see also* CTIA Comments at 39-40 (recommending excluding entities otherwise prohibited from federal procurement from the labeling program).

an agency charged with making national security determinations that a company's products lack the indicia of trustworthiness that the Cyber Trust Mark is intended to represent. Our action here thus supports and reinforces the steps we have taken in other proceedings to safeguard consumers and communications networks from equipment that poses an unacceptable risk to national security and that other federal agencies have taken to identify potential concerns that could seriously jeopardize the national security and law enforcement interests of the United States.[134]

34. With the exception of China's comments raising the same WTO issue we rejected in the Report and Order applying the Covered List to the FCC equipment authorization program,[135] the record overwhelmingly supports excluding from the IoT Labeling Program these products and devices produced by companies identified on the Covered List.[136] Additionally, USTelecom, CTIA, CTA, Cybersecurity Coalition and Consumer Reports specifically support excluding from the IoT Labeling Program IoT devices that are manufactured by companies on the Covered List,[137] but also urge the Commission to restrict any equipment manufactured by companies on additional federal restricted lists, including those otherwise banned from federal procurement.[138] Consumer Reports agrees with excluding systems that include components included on the Covered List or similar lists from the IoT Labeling Program.[139] Each of these lists represent the determination by relevant Federal agencies that the entities on the list may pose a national security threat within their respective areas, and as such we find that we cannot separately sanction their products as trustworthy via the IoT Labeling Program. While each list is designed to support specific prohibitions, their use here only excludes their contents from a voluntary program representing U.S. Government assessment of their security and does not prohibit any other use. Insofar as

[134] *See, e.g.*, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Third Report and Order, WC Docket No. 18-89 (Jul. 14, 2021); *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*, Report and Order, Order, and Further Notice of Proposed Rulemaking, ET Docket No. 21-232 and EA Docket No. 21-233 (Nov. 25, 2022).

[135] *See 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*, Report and Order, Order, and Further Notice of Proposed Rulemaking, ET Docket No. 21-232 and EA Docket No. 21-233, at 255 (Nov. 25, 2022).

[136] *See* ioXt Alliance Comments at 11-12; CTIA Comments at 39-41; NCTA Comments at 8; Somos Comments at 3; Kaiser Permanente Comments at 3; CTA Comments at 26; Consumer Reports Comments at 10; ITI Comments at 5-6; USTelecom Comments at 2,7; Cybersecurity Coalition Comments at 4-5; CTIA Reply Comments at 6. *But see* People's Republic of China Comments at 6 (claiming WTO Article 2.1 requires equally favorable treatment preventing any restrictions based on the Covered List).

[137] USTelecom Comments at 7-8; CTIA Comments at 39-41; CTA Comments at 26; Cybersecurity Coalition Comments at 4-5; Consumer Reports Comments at 10.

[138] *See* USTelecom Comments at 7-8 (Commission should also exclude devices on the following lists: FY2019 NDAA § 889; FAR § 52.204-25 (ban on federal procurement of certain equipment produced by Huawei, ZTE, Hytera, Hikvision, Dahua); FY2023 NDAA § 5949 (ban on federal procurement of semiconductor products and services from SMIC, CXMT, and YMTC); FAR § 52.204-23 (ban on federal procurement of Kaspersky Lab software and hardware); Bureau of Industry and Security, U.S. Department of Commerce, Supplement No. 4 to Part 744 – Entity List (2023), https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file [https://perma.cc/STW5-B8GW]; U.S. Department of Defense, Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. ("Mac") Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283), Tranche 2 (2022), https://media.defense.gov/2022/Oct/05/2003091659/-1/-1/0/1260H%20COMPANIES.PDF [https://perma.cc/5LMA-LZLG]); *see also* CTIA Comments at 39-41 (recommending entities otherwise banned from federal procurement should also be excluded from the program); CTA Comments at 26; Cybersecurity Coalition Comments at 4-5.

[139] Consumer Reports Comments at 10.

the FCC IoT Label reflects the FCC's signal to consumers about cybersecurity, it is reasonable for the FCC to take a cautious approach especially for those products for which relevant Federal agencies have expressed other security concerns.

35. *Applicant Declaration Under Penalty of Perjury*. To implement the Commission's goal of ensuring the Cyber Trust Mark is not affixed to products that pose a risk to national security or a risk to public safety, we require applicants seeking authorization to use the FCC IoT Label to provide an unsworn declaration under penalty of perjury that, all of the following are true and correct:[140]

(i) The product for which the applicant seeks to use the FCC IoT Label through cybersecurity certification meets all the requirements of the IoT Labeling Program.

(ii) The applicant is not identified as an entity producing covered communications equipment on the Covered List,[141] established pursuant to § 1.50002 of the of the Commission's rules.

(iii) The product is not comprised of "covered" equipment on the Covered List.

(iv) The product is not produced by any entity, its affiliates, or subsidiaries identified on the Department of Commerce's Entity List, or the Department of Defense's List of Chinese Military Companies.

(v) The product is not owned or controlled by or affiliated with any person or entity that has been suspended or debarred from receiving federal procurements or financial awards, to include all entities and individuals published as ineligible for award on the General Service Administration's System for Award Management.

36. If any applicant fails to make any of the above disclosures within 20 days after being notified of its noncompliance, such failure would result in termination of any improperly granted authorization to use the Label, and/or subject the applicant to other enforcement measures. The applicant is required to update its declaration, or withdraw a not-yet granted application, if any of the applicant's circumstances impacting the declarations materially change while the application is pending.

37. *Wireless Consumer IoT Devices vs. Wired Consumer IoT Devices*. Today's Order adopts the *IoT Labeling NPRM*'s proposal that the IoT Labeling Program apply initially to wireless consumer IoT devices. This is consistent with the *IoT Labeling NPRM* proposal to focus the scope of the IoT Labeling Program on intentional radiators that generate and emit RF energy by radiation or induction and exclude wired-only IoT devices,[142] noting such devices are encompassed by the Commission's section 302 authority governing the interference potential of devices that emit RF energy and can cause harmful interference.[143] We find that this distinction is appropriate, both because of the Commission's interest in keeping the scope of the IoT Labeling Program clear and manageable during its debut and because there is support in the record for wireless intentional radiators as most prevalent types of consumer IoT devices contemplated in the *IoT Labeling NPRM.* While we recognize that there are other types of RF devices – both unintentional and incidental radiators – that are subject to our jurisdiction, we are not including them in our IoT Labeling Program at this time.

38. We acknowledge there is substantial support in the record for including wired IoT

[140] 47 CFR § 1.16.

[141] 47 U.S.C. § 150001(c)(d) any equipment used in fixed and mobile networks that provides advanced communication service, provided the equipment includes or uses electronic components that is included on the Covered List.

[142] *IoT Labeling NPRM* at 7, para. 12.

[143] 47 U.S.C. § 302a(a)(1) ("The Commission may, 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; . . .").

consumer products within the scope of the IoT Labeling Program. Consumer Reports recommends including both wired and wireless IoT within the scope of the IoT Labeling Program, pointing out that wired IoT devices or products are vulnerable to cybersecurity threats just as wireless IoT devices or products are.[144] Consumer Reports also points out that "while wireless devices are the majority of IoT devices, there are still almost 700 million wired IoT devices globally, and they are expected to grow by a 10% [compound annual growth rate] through 2027 according to IoT Analytics 'State of IoT – Spring 2023 Report.'"[145] TÜV SÜD also encourages the Commission to cover both wired and wireless devices within the scope of the IoT Labeling Program,[146] and AIM emphasizes the importance of the security of both wired and wireless IoT to the cybersecurity ecosystem.[147] CTA further states that the Commission should not define the scope of the IoT Labeling Program in such a way as to exclude wired IoT products.[148] AHAM points out that both wired and wireless IoT are included in the NIST definition.[149]

39. While we agree that wired IoT products are susceptible to cyberattacks and similarly pose security risks to consumers and others, we find it to be in the public interest for the IoT Labeling Program to start with wireless consumer IoT products in view of the record indicating that "wireless devices are the majority of IoT devices,"[150] which would indicate that a focus on this product segment will have a substantial impact on the overall IoT market. The record also supports this approach, with Keysight Technologies, Inc. concurring that "the program should include consumer RF IoT products initially."[151] Further, we do not agree with arguments that there may be an unintended perception that "[c]reating a program that would only certify wireless IoT devices would send an improper message that only wireless IoT devices are secure."[152] Instead, we believe that beginning with wireless IoT products is both feasible and can be adopted with more speed, providing more prompt benefit in the marketplace. Further, a more limited scope will streamline the initial rollout of the IoT Labeling Program, provide focus to the additional tasks necessary to stand up the program, and lay the groundwork for expansion, and we do not foreclose consideration including wired IoT products in the future. As such and as discussed below, we also defer consideration of our legal authority to consider wired products at this time.[153]

C. Oversight and Management of the IoT Labeling Program

1. Fostering Close Public-Private Collaboration

40. In the *IoT Labeling NPRM*, the Commission recognized that for a voluntary IoT Labeling Program to be successful, it must include a close partnership and collaboration between federal government, industry, and other stakeholders.[154] The record in this proceeding supports implementation of the IoT Labeling Program through public-private collaboration that leverages the expertise and existing

[144] Consumer Reports Comments at 4.

[145] Consumer Reports Reply at 3 (citing Satyajit Sinha, *State of IoT: Number of connected IoT devices growing 16% to 16.7 billion globally* (May 24, 2023), https://iot-analytics.com/number-connected-iot-devices/ [https://perma.cc/E2NM-KB4Q]).

[146] TÜV SÜD Comments at 2.

[147] AIM Comments at 2, 5.

[148] CTA Comments at 13.

[149] AHAM Comments at 4.

[150] Consumer Reports Reply at 3.

[151] Keysight Technologies, Inc. Comments at 1 (Keysight).

[152] Planar Systems, Inc. Comments at 1 (Planar).

[153] *See infra* Section IV.

[154] *IoT Labeling NPRM* at 9, para. 19.

frameworks of the federal government, industry, and other stakeholders.[155] The *IoT Labeling NPRM* sought comment on adopting NIST's recommendation that there be one "scheme owner" ultimately responsible for overseeing and managing the IoT Labeling Program, and whether that entity should be the Commission. The Commission also sought comment on whether one or more third-party administrator(s) could be utilized to manage some or all of the IoT Labeling Program functions identified by NIST and, if so, which functions, and how such third-party administrators should be chosen.[156] Based on the comments filed regarding oversight and management of the IoT Labeling Program, the Commission finds it is in the public interest to continue to foster public-private collaboration, including with regard to the management and administration of the IoT Labeling Program, while ensuring the Commission retains ultimate control and oversight of the IoT Labeling Program. In this respect, providing a broad, unifying government oversight framework for existing private labeling schemes and other private efforts in this context will allow current participants in this ecosystem to capitalize on their existing investments and relationships in a way that not only promotes the overall effectiveness of the FCC's IoT Labeling Program and increases the security of the IoT ecosystem.

41. The Commission adopts the *IoT Labeling NPRM* proposal that the IoT Labeling Program be comprised of a single "program owner" responsible for the overall management and oversight of the IoT Labeling Program, with administrative support from one or more third party administrators.[157] NIST's white paper recommends one "scheme owner" responsible for managing the labeling program, determining its structure and management, and performing oversight to ensure the program is functioning consistently in keeping with overall objectives.[158] We agree that it is appropriate for a single entity to perform these functions, and find that the Commission will be the program owner of the IoT Labeling Program, and as such retains ultimate control over the program, and determines the program's structure. CSA highlights support in the record for having the Commission as the program owner, arguing that "[p]lacing the regulatory authority in the hands of the Commission and providing government-backed endorsement may strengthen trust with Consumers."[159] However, the *NIST Cybersecurity White Paper* also recommends the "scheme owner" be responsible for defining the conformity assessment requirements, developing the label and associated information, and conducting consumer outreach and education.[160]

42. While the Commission as program owner will *oversee* the elements of the program, the program will be supported by Cybersecurity Label Administrators (Label Administrators or CLAs) who will manage certain aspects of the program and authorize use the FCC IoT Label as well as a Lead Administrator selected by the Bureau from among the CLAs, which will undertake additional duties including acting as the point of contact between the CLAs and the Commission. In addition, the Commission believes it is appropriate for a Lead Administrator, in collaboration with stakeholders, to identify or develop, and recommend to the Commission for approval, the IoT specific standards and testing procedures, as well as design and placement of the label. The Lead Administrator will also be responsible for developing, in coordination with stakeholders, a consumer education plan and submitting the plan to the Bureau and engaging in consumer education. Each of these duties are discussed in depth

[155] CTA Comments at 16; ioXt Alliance Comments at 2; Kaiser Permanente Comments at 4.

[156] *IoT Labeling NPRM* at 10-11, para. 22.

[157] *Id.*

[158] *NIST Cybersecurity White Paper* at 2.

[159] CSA Reply at 4 (citing American Association for Laboratory Accreditation (A2LA) Comments at 2, TIC Comments at 3-4, Kaiser Permanente Comments at 3-4, UL Solutions Comments at 2-3, ITI Comments at 6, and Consumer Reports Comments at 10-12 to support Commission as program owner; Cybersecurity Coalition Comments at 5-6, and NEMA Comments at 6 as supporting the Commission overseeing and managing the IoT Labeling Program; and A2LA Comments at 2, 22, TIC Comments at 3-4, and Cybersecurity Coalition Comments at 5-6 as support for its argument that government-backed endorsement strengthening consumer trust).

[160] *NIST Cybersecurity White Paper* at 2.

below. The Cybersecurity Coalition recommends the Commission utilize a single administrator, rather than multiple administrators "to reduce the likelihood of conflict among administrators and simplify engagement with manufacturers, consumers, and government agencies."[161] CTA, on the other hand, contemplates multiple administrators, suggesting that the Commission may consider leveraging "a consortium of scheme owners[] to ensure that the IoT Labeling Program is administered and issues are adjudicated in an effective, objective, and timely fashion."[162] We agree with CTA's reasoning, while also acknowledging the Cybersecurity Coalition's concern regarding potential conflict. Accordingly, the Bureau will select a Lead Administrator from among the CLA applicants to address conflicts.

43. As an initial matter, we have looked to the structure of, and experiences with, the Commission's equipment authorization program and rules in developing the IoT Labeling Program, as proposed and discussed in the *IoT Labeling NPRM*. We emphasize, however, that the IoT Labeling Program is new and distinct, and it will operate under its own rules and with new authorities specifically delegated to PSHSB. This is consistent with the record developed in the proceeding, in which many commenters urged the Commission to keep the equipment authorization and IoT Labeling programs separate.[163] In addition, several commenters addressed whether obtaining a valid equipment authorization should be a pre-requisite for obtaining the Cyber Trust Mark,[164] or whether obtaining approval to use the Cyber Trust Mark would be required as a condition for applying for an equipment authorization.[165] We emphasize that our IoT Labeling Program is voluntary, and parties are required to follow the Commission's equipment authorization program regardless of whether or not they choose to participate in the IoT Labeling Program. We also clarify that there is no requirement to complete the equipment authorization process before qualifying for the Cyber Trust Mark;[166] however, our existing part 2 rules will continue to prohibit the marketing of a device that does not have a valid equipment authorization.[167]

44. We conclude that it is in the public interest and supported in the record to adopt the IoT Labeling Program structure recommended by NIST, with the modifications discussed above regarding third party administrators that are overseen by the Commission as the program owner. This and the following paragraph preview the remaining roles and responsibilities for the IoT Labeling Program, which will be developed in depth in the remaining sections of this Order. The Commission also will be responsible for coordinating mutual recognition of the Cyber Trust Mark with international partners, coordinating with the Lead Administrator, federal partners, industry, and other stakeholders on consumer education programs, and performing oversight to ensure the IoT Labeling Program is functioning properly. In addition, the Commission will specify the data to be included in a consumer-friendly registry that provides additional information about the security of the products approved to use the Cyber Trust Mark and is accessible through the QR Code that is required to accompany the Cyber Trust Mark. Further, the Commission will own and maintain the registration for the Cyber Trust Mark, which may only be used when the product has been appropriately tested and complies with the Commission's IoT Labeling Program requirements.

[161] Cybersecurity Coalition Comments at 5.

[162] CTA Comments at 23.

[163] *See, e.g.,* ITI Comments at 4; Consumer Reports Comments at 35; CTA Reply at 10; Letter from Association of Home Appliance Manufacturers, Connectivity Standards Alliance, Consumer Technology Association, CTIA Information Technology, Industry Council, National Electrical Manufacturers Association, Plumbing Manufacturers International Power Tool Institute, Security Industry Association, Telecommunications Industry Association, U.S. Chamber of Commerce, and USTelecom, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 23-239, at 1 (Nov. 8, 2023) (Coalition Letter Reply).

[164] NCTA Reply at 6; Coalition Letter Reply at 1.

[165] TIA Comments at 2; CTA Comments at 9.

[166] *See* Coalition Letter Reply at 1.

[167] *See* 47 CFR pt. 2.

45. The Commission will approve qualified Cybersecurity Label Administrators (Label Administrators or CLAs) to manage certain aspects of the labeling program and be authorized by the Commission to license the Cyber Trust Mark to manufacturers whose products are in compliance with the Commission's IoT cybersecurity labeling rules. The Commission will also select a Lead Administrator, which will be responsible for carrying out additional administrative responsibilities, including but not limited to reviewing applications and recognizing qualified and accredited Cybersecurity Testing Laboratories (CyberLABs) and engaging in consumer education regarding the Cyber Trust Mark. The Lead Administrator will also collaborate with cyber experts from industry, government, academia and other relevant sectors if needed to identify, develop, and maintain consumer IoT cybersecurity technical and conformity assessment standards that will be submitted to PSHSB for consideration and approval, and, subject to any required public notice and comment, incorporation in the Commission's rules by reference. The standards and testing procedures developed or identified in collaboration with stakeholders and submitted by the Lead Administrator for consideration by the Commission will, in turn, be used by accredited[168] testing labs recognized by the Lead Administrator—whether CyberLABs,[169] a CLA-run lab, or a testing lab internal to a company (in-house testing lab) for product testing.

46. Retaining key overarching functions within the Commission as discussed above will ensure the effective administration and oversight of this government program and protect the integrity of the FCC-owned Cyber Trust Mark, while perpetuating, where appropriate, the relevant efforts of the private sector that meet the goals and requirements of the program. We also agree with CSA that program ownership by the Commission will increase consumer confidence in the Cyber Trust Mark. In addition, the clear high-level oversight functions retained for the Commission ensures the Commission has meaningful decision making control.[170] Here, while the CLA(s) will recommend standards and testing procedures to be approved by the Commission as well as manage the day-to-day administrative functions assigned, the Commission will ultimately review, consider, and exercise judgment on whether the requirements are appropriate to support the Commission's program, and on how the program is ultimately administered.

2. Cybersecurity Label Administrators (CLAs)

47. The *IoT Labeling NPRM* sought comment on how one or more third-party administrators might be used to manage some or all of the labeling program functions and the best ways for the Commission to utilize the respective expertise of the Commission, other federal government entities,

[168] The organization(s) accrediting the prospective Label Administrators and testing labs must meet the requirements and conditions in ISO/IEC 17011. *See* 47 CFR § 8.910(b)(1) ISO/IEC 17011:2004(E), "Conformity assessment—General requirements for accreditation bodies accrediting conformity assessment bodies," First Edition, 2004–09–01, IBR approved for §§ 8.216(e) and 8.217(b).

[169] There appeared to be some confusion in the record with the Commission's use of the term Cybersecurity Labeling Authorization Bodies. Specifically, the ANSI National Accreditation Board (ANAB) recommended the Commission reconsider the use of the term "CyberLAB" as the "implication that such organizations are laboratories could create market confusion." ANAB Reply at 2. We disagree that the term CyberLAB may be confusing because these organizations are, in fact, laboratories/testing bodies that will be testing products to determine compliance with applicable standards. The CyberLABs, however, are not "certification bodies." Rather, the entity that will be authorizing an applicant to use the Cyber Trust Mark on their product is the CLA, as described in para. 55, *infra*. To ensure there is no confusion, the Commission has changed the term from Cybersecurity Labeling "Authorization Bodies" as these terms are reserved for accreditation bodies, to Cybersecurity Testing Laboratories, reflecting that the function of these labs is for testing and generating reports, and not certifying or issuing a label. We continue to use the short-form term "CyberLAB" to refer to these testing labs.

[170] *Consumers' Rsch. v. FCC*, 88 F.4th 917, 926 (11th Cir. 2023) ("[A]government agency may delegate statutory authority to private entities without violating the private nondelegation doctrine so long as (1) the entity "function[s] subordinately" to the agency, and (2) the agency retains "authority and surveillance over the activities" of the private entity.").

industry, and other stakeholders.[171] It also sought comment on how the Commission might select one or more third-party administrators, what qualifications such administrators should possess, what national security considerations are relevant to these qualifications, and whether there are existing stakeholders well-suited to convene the working group the Commission tasks with developing and identifying IoT security standards.[172]

48. We adopt the *IoT Labeling NPRM's* proposal that one or more qualified third party administrators (Cybersecurity Labeling Administrators or CLAs) be designated by the Commission to manage certain aspects of the labeling program and be authorized to certify the application of the FCC IoT Label by manufacturers whose products are found to be in compliance with the Commission's IoT cybersecurity labeling rules and regulations.[173] The record supports the Commission's adoption of a labeling program that is supported by CLAs.[174] According to TIC Council Americas, involving independent third party administrators who verify that labeled products meet the program requirements will bring trust, consistency, and an impartial level playing field to the Cyber Trust Mark.[175] The Cybersecurity Coalition, Widelity, and CSA highlight that utilizing experienced third party administrators will allow the program to run more efficiently and will provide "the required expertise for the administration of the program."[176] CTA and other commenters also assert that the IoT Labeling Program will be best served if the Commission "leverage[s] the unique expertise and existing certification infrastructure offered by well-regarded industry organizations."[177] AHAM says that "[g]iven the volume and increasing numbers of IoT products on the market, [the] FCC needs to give manufacturers as many options as possible as far as obtaining the Cyber Trust mark" and that "third parties will play an important role in any successful program."[178]

49. CTA supports assigning certain responsibilities to one or more independent, (i.e., neutral) third party administrators which it refers to as "Authorized Scheme Owners." However, the Commission disagrees with this descriptor insofar as some commenters are confused as to whether the "scheme owner" is the entity ultimately responsible for the program, or a third party entity responsible for certain program administration functions or specified tasks under the ultimate direction of the Commission. To avoid confusion, the Commission refers to these third-party administrators as CLAs. These CLAs are neutral third parties independent of the applicant and within the context of a program overseen by the Commission.

50. We believe that authorizing one or more CLAs to handle the routine administration of the program will help to ensure a timely and consistent rollout of the program. In particular, several private entities have already implemented robust IoT cybersecurity labeling programs with established business processes in place to receive applications from IoT manufacturers and conduct conformity/standards

[171] *IoT Labeling NPRM* at 11, para. 23.

[172] *Id.* at 11, paras. 23-24.

[173] CTA Comments at 10; *but see* Kaiser Permanente Comments at 3 (supporting use of third parties to play integral roles in the management and administration of the IoT Labeling Program, subject to the FCC maintaining oversight of the program and serving as the entity that grants permission to use the Cyber Trust Mark to applicants).

[174] *See, e.g.*, CTA Reply at 7; CTA Comments at 16-18; ioXt Alliance Comments at 13; UL Solutions Comments at 6; CTIA Comments at 26-27; Cybersecurity Coalition Comments at 5; ITI Comments at 8.

[175] TIC Council Americas Comments at 1.

[176] Cybersecurity Coalition Comments at 5-6; Widelity Comments at 3; CSA Comments at 5-6.

[177] CTA Comments at 10; *see also* AHAM Comments at 3; Cybersecurity Coalition Comments at 5; ioXt Alliance Comments at 13; UL Solutions Comments at 6.

[178] AHAM Comments at 3; *see also* Kaiser Permanente Comments at 3 ("Given the wide scope of IoT devices and products eligible for the Program, we recommend considering the use of multiple third-party administrators to share responsibilities and manage the day-to-day details of the application, assessment, granting and maintenance/renewal processes for defined subsets of IoT devices.").

testing against widely accepted cybersecurity guidelines (e.g., NIST guidelines) or proprietary product profiles based on the NIST criteria.[179] We anticipate a large number of entities will seek grants of authorization to use the FCC IoT Label and we are concerned that if we were to adopt a program limited to a single administrator, there may be bottlenecking delays in the processing of applications and a single administrator could result in a single point of failure in the program. Allowing multiple CLAs to execute the role of day-to-day administration of the program will provide for the simultaneous processing of a significant number of applications, provide redundancy of structure, and potentially foster competition in this space to better serve those seeking access to the label. In addition, leveraging the expertise of multiple existing program managers and using pre-existing systems and processes that meet our program specifications will minimize administrative delay, while promoting an efficient and timely rollout of the Cyber Trust Mark. This will also ensure that the Commission effectively utilizes the expertise of those entities who have made investments in their own cybersecurity labeling programs and have experience working with manufacturers and IoT conformity and standards testing, expediting the ability to provide consumers with a simple way to understand the relative security of the products and devices they purchase under a government-backed standard.

3. Responsibilities of the Lead Administrator and CLAs

51. We recognize, however, that there is a need for a common interface between the CLAs and the Commission to facilitate ease of engagement and to conduct other initial tasks associated with the launch of the program.[180] We delegate authority to PSHSB to review CLA applications, review CLA applications that also request consideration for Lead Administrator, select the Lead Administrator and manage changes in the Lead Administrator.

52. *Lead Administrator Duties*. The Lead Administrator will undertake the following duties in addition to the CLA duties outlined below:

a. interface with the Commission on behalf of the CLAs, including but not limited to submitting to the Bureau all complaints alleging a product bearing the FCC IoT Label does not meet the requirements of the Commission's labeling program;

b. conduct stakeholder outreach as appropriate;

c. accept, review, and approve or deny applications from labs seeking recognition as a lab authorized to perform the conformity testing necessary to support an application for authority to affix the FCC IoT Label,[181] and maintain a publicly available list of Lead Administrator-recognized labs and a list of labs that have lost their recognition;

d. within 90 days of release of the Public Notice announcing the Lead Administrator selection, the Lead Administrator shall, in collaboration with stakeholders (e.g., cyber experts from industry, government, and academia) as appropriate:

    i. submit to the Bureau recommendations identifying and/or developing the technical standards and testing procedures for the Commission to consider with regard to at least one class of IoT products eligible for the IoT Labeling Program. The Bureau will evaluate the recommendations, and if the Bureau approves of the recommendations, subject to any required public notice and

[179] CTA Comments at 16; ioXt Alliance Comments at 2-3 (referencing the ioXt Certification Program).

[180] *See* ioXt Alliance Comments at 13 (suggesting a lead entity to oversee operation by recommending the FCC "consider establishing an advisory committee/board to advise on operations of the program.").

[181] If the Lead Administrator, in addition to its administrative duties, intends to offer lab testing service (CLA-run lab), it must submit an application with PSHSB seeking FCC recognition as a lab authorized to perform conformity testing to support an application for authority to affix the FCC IoT Label. The Lead Administrator is not authorized to recognize its own cybersecurity testing lab. If approved by PSHSB, the Lead Administrator will add the name of its lab to the list of recognized labs.

comment, incorporate them by reference into the Commission's rules;

ii. submit to the Bureau a recommendation on how often a given class of IoT products must renew their request for authority to bear the FCC IoT Label, which may be dependent on the type of product, and that such a recommendation be submitted in connection with the relevant standards recommendations for an IoT product or class of IoT products;[182] The Bureau will evaluate the recommendations, and if the Bureau approves of the recommendations, subject to any required public notice and comment, incorporate them by reference into the Commission's rules; and

iii. submit to the Bureau recommendations on the design of the FCC IoT Label, including but not limited to labeling design and placement (e.g., size and white spaces, product packaging.) The Bureau will evaluate the recommendations, and if the Bureau approves of the recommendations, subject to any required public notice and comment, incorporate them by reference into the Commission's rules.

e. submit to the Commission reports on CLAs' post-market surveillance activities and findings in the format and by the date specified by PSHSB;

f. develop in collaboration with stakeholders a consumer education campaign, submit the plan to the PSHSB, and participate in consumer education;[183]

g. receive complaints about the Labeling Program, including but not limited to consumer complaints about the registry and coordinate with manufacturers to resolve any technical problems associated with consumers accessing the information in the registry;

h. facilitate coordination between CLAs; and

i. submit to the Commission any other reports upon request of the Commission or as required by Commission rule.

53. *Cybersecurity Label Administrator Duties.* CLA(s) are responsible for various administrative duties, including:

a. receive and evaluate applications and supporting data requesting authority to use the FCC IoT Label on the product subject to the application;

b. grant an application only if it meets all of the Commission's requirements to use the FCC IoT Label and authorize (i.e., certify) the applicant to use the FCC IoT Label on the product subject to the application;

c. ensure that manufacturers make all required information accessible by the IoT registry;

d. participate in consumer education campaign in coordination with the Lead Administrator;

e. perform post-market surveillance activities, such as audits, in accordance with ISO/IEC 17065[184] and submit periodic reports to the Lead Administrator of their

[182] *See infra* para. 124.

[183] *See infra* Section III.L.

[184] *See* 47 CFR § 8.910(b)(3); ISO/IEC 17065:2012(E), "Conformity assessment—Requirements for bodies certifying products, processes and services," First Edition, 2012–09–15, IBR approved for §§ 8.218(b), 8.219(b), (c),

(continued….)

post-market surveillance activities and findings in the format and by the date specified by PSHSB; and

f. receive complaints alleging an IoT product does not support the cybersecurity criteria conveyed by the Cyber Trust Mark and refer these complaints to the Lead Administrator which will notify PSHSB.[185]

54. The record supports the use of CLAs to support a variety of tasks within the program's construct. ioXt Alliance supports utilizing CLAs for evaluating and certifying products for the Cyber Trust Mark.[186] CTA supports utilizing CLAs to conduct program operations.[187] The Cybersecurity Coalition and Kaiser Permanente also support utilizing CLAs for managing the day-to-day operations of the IoT Labeling Program.[188] CSA argues that, "the day-to-day administration of the Cyber Trust Mark Program should be managed by a Third-Party Administrator, serving as the entity that grants permission to use the Program trademark to applicants."[189] In addition, ITI recommends that it should be the responsibility of the CLA to review or audit self-attestations and that "third-party administrators can and should play a key role in administering conformity assessment schemes."[190] CSA and CTIA further recommend adopting the *IoT Labeling NPRM's* proposal that a third party administrator evaluate, accredit, or recognize the CyberLABs,[191] and CSA also "recommends that the Commission hire a third-party administrator to operate the IoT Registry."[192] Finally, ioXt Alliance recommends that third party administrators should also "vet companies and products during the certification process"[193] to determine which products pose a threat to national security, based on Commission guidance. ioXt Alliance also notes in its comments that the "label design and associated information should be informed by the expertise of manufacturers and third-party administrators."[194]

55. Subject to Commission oversight, and consistent with recommendations in the record, the CLAs will evaluate and grant or deny requests for authority to use the FCC IoT Label on consumer IoT products in accordance with the IoT Labeling Program. Each administrator will be responsible for certifying that the consumer IoT products for which it authorizes a manufacturer to apply the FCC IoT Label are tested by an accredited testing lab, which as discussed further below may be a CyberLAB, the applicant's own in-house lab, or a CLA-run lab, and that the testing report demonstrates the product conforms to all Commission IoT labeling rules. The CLA will track each application it receives requesting authority to use the FCC IoT Label, and the disposition of all applications, including date of filing, date of acceptance as complete, the date and reason application is returned to applicant, and date of grant or denial. The CLAs will review each application they receive to ensure the application and

(d), (f), and (g). ISO/IEC 17065:2012, *Conformity Assessment – Requirements for Bodies Certifying Products, Processes and Services*, https://anab.ansi.org/standard/iso-iec-17065/ [https://perma.cc/8LLA-MQ39].

[185] This process does not foreclose the ability of consumers to file an informal complaint in accordance with the Commission's rules. *See* 47 CFR §§ 1.716 – 1.719. In the event an informal complaint is filed with the Commission, the complaint will be forwarded to the Lead Administrator for investigation and/or referral to the issuing CLA.

[186] ioXt Alliance Comments at 14.

[187] *See* CTA Reply at 4.

[188] *See* Cybersecurity Coalition Comments at 5; Kaiser Permanente Comments at 3.

[189] CSA Reply at 5-6 (citing Kaiser Permanente Comments at 3-4; ITI Comments at 6).

[190] ITI Comments at 9.

[191] CTIA Comments at 26 (citing *IoT Labeling NPRM* at 12, para. 26).

[192] CSA Comments at 15.

[193] ioXt Alliance Comments at 12.

[194] *Id.* at 13.

supporting documents are provided and are sufficient to show the product conforms to all Commission rules and that it includes a compliance test report generated by an accredited and Lead Administrator-recognized testing lab (e.g., third party lab (CyberLAB), applicant's in-house testing lab, or CLA-run lab). If the application is deficient, it will not be granted until all necessary conditions are satisfied. If the application is complete and meets all of the Commission's requirements, the CLA will issue a cybersecurity labeling authorization (i.e., cybersecurity certification) approving the applicant to affix the FCC IoT Label to the identified product.

56. In addition to its role as a CLA, the Lead Administrator may collaborate with stakeholders (e.g., cyber experts from industry, government, and academia) as appropriate to develop or identify, and maintain, consumer IoT cybersecurity technical and conformity assessment standards to be met for each class of IoT product seeking authority to affix the FCC IoT Label on their product, which the Lead Administrator will submit to PSHSB for consideration and approval and, subject to any required public notice and comment, incorporation in its rules by reference. Adopting standards through consensus is supported by the record in this proceeding.[195] The Information Technology Industry Counsel (ITI) supports the Commission retaining ownership of the IoT Labeling Program and authorizing the "various industry-led, consensus standards, which can be used to gain approval for the Cyber Trust Mark."[196] ITI also notes that using industry-led, consensus standards will also limit the likelihood of legal challenges.[197] UL Standards & Engagement agrees that the FCC should use a "voluntary consensus-based standards development process" to create and update standards for the IoT Labeling Program.[198] The U.S. Chamber of Commerce also supports a consensus-based approach urging the Commission "to track closely with public-private developments in IoT cybersecurity as well as industry-driven initiatives, such as the *C2 Consensus on IoT Device Security Baseline Capabilities* (C2 Consensus)[199] and CTIA's cybersecurity certification program for IoT devices."[200] The Council to Secure the Digital Economy (CSDE), which is "composed of USTelecom, the Consumer Technology Association (CTA), and 13 global information and communications technology (ICT) companies - has also already convened technical experts from 19 leading organizations throughout the ICT sector to develop and advance industry consensus on baseline security capabilities for new devices,"[201] including the C2 Consensus document, which provides guidance to the public and private sectors on IoT devices security.[202] We agree with these recommendations that the Commission adopt standards following recommendations based on an industry-led consensus process, leveraging standards work already in process or completed, which will

[195] As below, we emphasize the importance of leveraging existing expertise in this space, and as such adopt as a criterion for consideration in selecting the lead administrator the ability to convene and develop consensus among stakeholders.

[196] ITI Reply at 5.

[197] *Id.* at 6.

[198] UL Standards & Engagement Comments at 1.

[199] Council to Secure the Digital Economy, C2 Consensus on IoT Device Security Baseline Capabilities (2019), https://kvh31b.p3cdn1.secureserver.net/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf [https://perma.cc/6HTV-25ZP]; Council to Secure the Digital Economy, The C2 Consensus on IoT Device Security Baseline Capabilities – 2021 Supplement (2021), https://csde.org/wp-content/uploads/2021/04/C2-Tech-Report_2021_final.pdf [https://perma.cc/U45C-DGYT].

[200] U.S. Chamber of Commerce Comments at 3 (Chamber). The Chamber also argues that "[a]bove all, the Commission should reach a consensus with industry on fundamental concerns including the scope of covered IoT, security criteria and standards, conformity assessments, and liability protections." Chamber Comments at 3.

[201] Council to Secure the Digital Economy, The C2 Consensus on IoT Device Security Baseline Capabilities at 1 (2019), https://csde.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf [https://perma.cc/UG7K-C4RZ].

[202] *Id*.

provide for the swift development and implementation of the IoT Labeling Program.

57. The Lead Administrator is to base the recommended technical standards and testing procedures on the NISTIR 8425, *Profile of the IoT Core Baseline for Consumer IoT Products*. As noted by ITI, there is "a suite of existing standards that might be leveraged to ensure that the outcomes NIST outlines can be met."[203] In addition, NIST's *IoT Product Component Requirements Essay* provides a summary of standards and guidance that NIST has initially identified as applicable to IoT devices and IoT product components, that the Lead Administrator may determine are applicable to the IoT Labeling Program.[204] The Lead Administrator should evaluate and leverage existing work for efficiency and speed to market where appropriate in making its recommendations to the Commission.

58. The Lead Administrator in collaboration with stakeholders as appropriate will identify or develop IoT cybersecurity standards (or packages of standards) and testing procedures that they determine can be used to test that a product meets the NISTIR 8425 criteria for each class of products identified by the working group.[205] The Lead Administrator will submit to the Bureau recommendations on a rolling basis as they are identified, but shall submit the initial set of recommendations no later than 90-days after release of the Public Notice selecting the Lead Administrator. We specify a timeframe here to ensure timeliness of initial standards and prompt launch of the program. Noting the work already ongoing on these issues,[206] we also find such a timeframe to be reasonably achievable. The proposed standards (or packages of standards) and testing procedures must be approved by the Commission prior to implementation. The Commission delegates authority to PSHSB to evaluate and (after any required public notice and comment) approve (or not approve) the technical standards and testing procedures proposed by the Lead Administrator for use in the IoT Labeling Program and incorporate the approved standards and testing procedures by reference into the Commission's rules. The Commission further directs the Bureau to ensure the standards and testing procedures are relevant and appropriate to support the Commission's IoT Labeling Program.

4. Selecting CLAs and Revoking Authority to Grant Applications to Use the FCC IoT Label

59. *Selecting CLAs*. Each entity seeking authority to act as a CLA must file an application with the Commission for consideration by PSHSB,[207] which includes a description of its organization structure, an explanation of how it will avoid personal and organizational conflict when processing applications, a description of its processes for evaluating applications seeking authority to use the FCC IoT Label, and a demonstration of expertise that will be necessary to effectively serve as a CLA including, but not limited to:

1. Cybersecurity expertise and capabilities in addition to industry knowledge of IoT and IoT labeling requirements.

[203] ITI Reply at 5.

[204] NIST IoT Product Component Requirements Essay at 3-7.

[205] *See, e.g.*, CTIA Certification, *Cybersecurity Certification Program for IoT devices*, version 1.3 (July 2020), https://api.ctia.org/wp-content/uploads/2020/08/CTIA-IoT-Cybersecurity-Program-Management-Document-Ver-1.3.pdf [https://perma.cc/E8P6-9RV3].

[206] *See* Letter from David Grossman, Vice President, Regulatory Affairs, CTA, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 23-239, at 1-2 (Feb. 8, 2024).

[207] This approach necessitates a mechanism for the Commission to recognize administrators, and we accordingly adopt a rule doing so. *See infra* Appx. A, 47 CFR § 8.218. We model our approach on analogous elements of our equipment authorization rules, with which the Commission and industry have substantial experience, and which have proven workable in practice. *See* 47 CFR § 2.949. We delegate to PSHSB and OMD authority to take any necessary steps, including adoption of additional procedures and any applicable fees (pursuant to any required public notice and comment), as necessary to ensure compliance with the Communications Act with respect to any rules adopted here that contemplate the filing of applications directly with the Commission.47 U.S.C. § 158(c).

2. Expert knowledge of NIST's cybersecurity guidance, including but not limited to NIST's recommended criteria and labeling program approaches for cybersecurity labeling of consumer IoT products.

3. Expert knowledge of FCC rules and procedures associated with product compliance testing and certification.

4. Knowledge of Federal law and guidance governing the security and privacy of agency information systems.

5. Demonstration of ability to securely handle large volumes of information and demonstration of internal security practices.

6. Accreditation pursuant to all the requirements associated with ISO/IEC 17065[208] with the appropriate scope.[209] We recognize that CLAs cannot obtain accreditation to the FCC scope until after the Commission adopts standards and testing procedures. As such, the Commission will accept and conditionally approve CLA applications from entities that meet the other FCC program requirements and commit to obtain ISO/IEC 17065 accreditation with the appropriate scope within six (6) months of the effective date by the adopted standards and testing procedures. CLA approval to authorize use of the FCC IoT Label will be finalized upon receipt and demonstration to the Commission of ISO/IEC 17065 accreditation with the appropriate scope.[210]

7. Demonstrate implementation of controls to eliminate actual or potential conflicts of interests (including both personal and organizational), particularly with regard to commercially sensitive information, to include but not limited to, remaining impartial and unbiased and prevent them from giving preferential treatment to certain applications (e.g., application line jumping) and from implementing heightened scrutiny of applications from entities not members or otherwise aligned with the CLA.

8. That the applicant is not owned or controlled by or affiliated with any entity identified on the Commission's Covered List or is otherwise prohibited from participating in the IoT Labeling Program. We will dismiss all CLA applications from an entity (company) identified on the Commission's Covered List, the Department of Commerce's Entity List,[211] and the Department of Defense's List of Chinese Military Companies.[212]

9. That the applicant is not owned or controlled by or affiliated with any person or entity that has been suspended or debarred from receiving federal procurements or financial awards, to include all entities and individuals published as ineligible for award on the General Service

[208] ISO/IEC 17065:2012(E), "Conformity assessment—Requirements for bodies certifying products, processes and services," First Edition, 2012–09–15, IBR approved for §§ 8.950(b), 8.960(b), 8.962(b), (c), (d), (f), and (g). ISO/IEC 17065:2012, *Conformity Assessment – Requirements for Bodies Certifying Products, Processes and Services*, https://anab.ansi.org/standard/iso-iec-17065/ [https://perma.cc/8LLA-MQ39].

[209] The scope of CLA's ISO/IEC 17065 certification includes certifying IoT products and devices for compliance with FCC cybersecurity standards.

[210] Consistent with standard practice for accreditation, the organization accrediting the CLAs must be recognized by the Bureau to perform such accreditation based on International Standard ISO/IEC 17011. ISO/IEC 17011:2017.

[211] *See* Bureau of Industry and Security, U.S. Department of Commerce, Supplement No. 4 to Part 744 – Entity List (2023), https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file [https://perma.cc/STW5-B8GW].

[212] *See* Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. ("Mac") Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283), Tranche 2, U.S. Department of Defense (2022), https://media.defense.gov/2022/Oct/05/2003091659/-1/-1/0/1260H%20COMPANIES.PDF [https://perma.cc/5LMA-LZLG].

Administration's System for Award Management.[213]

10. In addition to completing the CLA application information, entities seeking to be the Lead Administrator will submit a description of how they will execute the duties of the Lead Administrator, including:

    a. their previous experience in IoT cybersecurity;

    b. what role, if any, they have played in IoT labeling;

    c. their capacity to execute the Lead Administrator duties outlined in this Order;

    d. how they would engage and collaborate with stakeholders to identify or develop the Bureau recommendations discussed in this Order;

    e. a proposed consumer education campaign; and

    f. additional information the applicant believes demonstrates why they should be the Lead Administrator.

60. For items #7 and #8, we note that the record raises national security considerations when selecting a Label Administrator. For example, CTIA urges that the Commission "exclude all entities on the Covered List (not just those included on the list for producing equipment), all entities on the other lists identified in the *IoT Labeling NPRM*, as well as entities that are otherwise banned from federal procurement."[214] CTIA explains that these broad exclusions for program participation are necessary because of "the unique nature of the proposed labeling program – namely that it is both government-administered and voluntary – counsels in favor of painting with a broad brush on national security-based exclusions."[215] We agree with the commenters in the record, and consistent with our reasoning herein addressing the exclusion of certain products that would raise potential national security concerns, we also prohibit entities owned or controlled by or affiliated with entities that produce equipment found on the Covered List, as well as entities specified on the other lists referenced above or those suspended or debarred from receiving federal procurements or financial awards from being a CLA in view of national security considerations and to insure the integrity of the IoT Labeling Program. Each of these lists represent the determination of relevant Federal agencies that the entities on the list may pose a national security threat within their respective areas, and as such we find that it is not in the public interest to permit these entities to provide assurance to the American public that products meets minimum cybersecurity standards. Importantly, we are only excluding the entities of the lists from a voluntary program under which the FCC approves their capability to oversee cybersecurity certification testing for purposes of the IoT Label. Insofar as the FCC IoT Label reflects the FCC's signal to consumers about cybersecurity, it is reasonable for us to take a cautious approach when approving entities to conduct the underlying product evaluations when relevant Federal Agencies have expressed security concerns with the entity.

61. NCTA also suggests that 'any "foreign entity of concern' as defined by the CHIPS Act should be ineligible for certification or recognition as a CyberLAB."[216] Further, ioXt Alliance recommends that the Commission "establish rules to ensure CyberLABs are not subject to undue influence by foreign adversaries."[217] We agree that it would be problematic for the U.S. to rely on the

[213] *See* U.S. General Services Administration System for Award Management, *Exclusion Types*, https://sam.gov/content/entity-information/resources/exclusion-types [https://perma.cc/5L45-LKCJ] (last visited Feb. 15, 2024).

[214] CTIA Reply at 7.

[215] CTIA Comments at 41.

[216] NCTA Comments at 8.

[217] ioXt Alliance Reply at 6.

determination of entities controlled or affiliated with "foreign adversaries" as to the security of products approved to use the Cyber Trust Mark, and therefore the FCC will not recognize for purposes of the IoT Labeling Program any applicant that is an entity, its affiliate, or subsidiary owned or controlled by a "foreign adversary" country. A "foreign adversary" country is defined in the Department of Commerce's rule, 15 CFR § 7.4,[218] and includes China (including Hong Kong), Cuba, Iran, North Korea, Russia, and Maduro Regime. We do not otherwise see a basis to preclude other foreign entities from serving as CLAs, but at this preliminary stage of establishing the IoT Labeling Program—where no international agreements are yet in place in this regard, and oversight details continue to be effectuated—we defer action in this regard. We delegate authority to PSHSB, in consultation with OIA, to evaluate and (after any appropriate public notice and comment) establish qualification criteria for any entity outside the United States to be approved to act as a CLA once any appropriate international agreements or other appropriate prerequisites are in place.

62. We decline to require that a CLA be a non-profit. In the *IoT Labeling NPRM*, we sought comment on whether the CLA should be required to be a non-profit entity.[219] The Cybersecurity Coalition recommends that the CLA be a non-profit entity, but did not elaborate on why, focusing their comments on having a neutral, independent third party that followed consistent pricing guidelines and had industry experience and strong security practices.[220] Researchers from the Northeastern University's College of Engineering similarly agreed that the Label Administrator should be a non-profit while emphasizing that the CLA should not have conflicts of interest.[221] We decline, however, to require that the CLA be a non-profit organization, recognizing that there may be well-qualified companies that may be for-profit organizations or non-profit organizations that possess the other relevant qualifications. We agree with what appear to be the underlying concerns of the record, that the CLA be neutral, have the knowledge outlined above, (e.g., knowledge regarding FCC rules, IoT cybersecurity standards and testing procedures), and be free of conflicts.[222] However, we believe that a company that satisfies the above requirements could carry out the CLA duties without being a non-profit organization. Moreover, expanding the pool of potential participants should increase the likelihood that a reasonable number of qualified entities apply to fulfill the specified roles. In addition, the record did not highlight reasons why a for-profit company would be incapable of fulfilling the role of label administrator.

63. Termination of CLA Authority. To address national security concerns, the authority of CLAs to grant applications to use the FCC IoT Label under the IoT Labeling Program will automatically terminate if the CLA subsequently becomes owned or controlled by or affiliated with an entity that produces equipment found on the Covered List, or otherwise added to any exclusionary list identified in this item as precluding authorization as a CLA. In addition, a CLA's authority may also be terminated for failure to uphold the required competencies or accreditations enumerated above. We delegate authority to

[218] 15 CFR § 7.4 (stating "[t]he Secretary has determined that the following foreign governments or foreign non-government persons have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons and, therefore, constitute foreign adversaries solely for the purposes of the Executive Order, this rule, and any subsequent rule" promulgated pursuant to the Executive Order); *see* 15 CFR § 7.2 ("Foreign adversary means any foreign government or foreign non-government person determined by the Secretary to have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons."); *see* Executive Order 13873 of May 15, 2019, Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 22689 (May 15, 2019).

[219] *IoT Labeling NPRM* at 11, para. 24.

[220] Cybersecurity Coalition Comments at 5.

[221] Northeastern University College of Engineering Comments at 3 ("Ideally, administrators should [be a] non-profit academia-based organization with connections to the industry but no conflict of interest.").

[222] *See, e.g.*, Cybersecurity Coalition Comments at 5; Northeastern University College of Engineering Comments at 3.

PSHSB, to determine if a CLA's authority is to be terminated in the latter circumstance, and to terminate such authorization.[223] PSHSB, may identify such CLA deficiencies itself or receive notice from other entities, including other agencies, consumers, and industry, that products granted authorization by a CLA do not accurately reflect the security posture of the product. Products authorized to use the FCC IoT Label by a disqualified CLA will be subject to the disqualification procedures described further below.

64. *CLA Application Filing Window*. We delegate authority to the Bureau to issue a Public Notice opening the initial filing window to receive applications from entities seeking authority to be recognized as a CLA (and Lead Administrator) under the IoT Labeling Program with instructions on how to apply and further details on the qualifications required of CLA applicants as well as the decision criteria used to select applicants. We also delegate to the Bureau authority to open additional filing windows or otherwise accept additional applications for authority to be recognized by the Bureau as a CLA when and as the Bureau determines it is necessary. Interested parties must establish they meet the requirements established in this Order. The Commission notes that it may refer applications to the U.S. Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Sector (Team Telecom) for their review and consideration of national security and law-enforcement risks.[224] We further delegate authority to PSHSB in coordination with the Office of the Managing Director (OMD) (specifically Office of the Chief Information Officer) and, to the extent necessary, the Office of General Counsel (OGC) (specifically the Senior Agency Official for Privacy), to receive and review each application for compliance with the criteria established in this order. We also delegate to PSHSB authority to adopt additional criteria and administrator procedures necessary to efficiently select one or more independent, non-governmental entities, to act as CLA(s). We delegate authority to PSHSB to release a Public Notice announcing the CLA(s) selected by the Bureau and next steps for each entity, including but not limited the execution of appropriate documentation governing the details of the CLA's responsibilities. Moreover, we delegate to PSHSB and OMD authority to take any necessary steps, including adoption of additional procedures and any applicable fees after selection of the CLAs, if necessary to ensure compliance with the Communications Act or applicable government-wide statutes that are implicated by the IoT Labeling Program. Finally, we also delegate authority to PSHSB and OMD, in consultation with OGC, to take any additional actions necessary to preserve the Commission's rights to the Cyber Trust Mark under trademark and other applicable laws. Only entities who have followed the procedures required by PSHSB and OMD and executed relevant required documentation will be authorized by the Commission to accept and grant applications authorizing the use of the FCC IoT Label, which includes the Cyber Trust Mark and QR Code.

D. CyberLABs, CLA-Run Labs, and In-House Testing Labs

65. The *IoT Labeling NPRM* sought comment on how IoT devices or products could demonstrate compliance with IoT security standards.[225] In the *IoT Labeling NPRM*, the Commission proposed the IoT Labeling Program could draw from the Commission's organizational structure for approving RF equipment when developing a process for assessing IoT devices and products for compliance with the IoT cybersecurity standards. In this case, the Commission proposed naming third parties with expertise in security and compliance testing to fill this role and proposed to call these entities

[223] Because of the public safety importance of a CLA having the requisite qualifications and adhering to our rules when evaluating requests to use the FCC IoT Label, this process should proceed appropriately expeditiously to minimize any periods of time where a CLA continues to operate in that capacity once concerns have come to PSHSB's attention. In particular, PSHSB shall provide notice to the CLA that the Bureau proposes to terminate the CLA's authority and provide the CLA a reasonable opportunity to respond (not more than 20 days) before reaching a decision on possible termination. PSHSB may suspend the CLA's ability to issues labeling authorizations during the pendency of such consideration if appropriate.

[224] *Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*, Order 36 FCC Rcd 14848 (2021).

[225] *IoT Labeling NPRM* at 11, para. 25.

CyberLABs.[226]

66. The Commission envisioned the role of CyberLABs as assessing IoT devices or products for compliance against IoT security standards, once developed.[227] The Commission sought comment on whether the Commission or one of the authorized label administrators would evaluate, accredit, or recognize the CyberLABs, noting that it was seeking to ensure that CyberLABs have the necessary expertise and resources to properly test and assess whether IoT devices and products are in compliance with the IoT security standards.[228] To become accredited and FCC-recognized for the proposed IoT Labeling Program, the Commission proposed the submission of applications demonstrating the applicant CyberLAB met the following requirements:

- Qualifications: The CyberLAB has technical expertise in cybersecurity testing and conformity assessment of IoT devices and products.
- Resources: The CyberLAB has the necessary equipment, facilities, and personnel to conduct cybersecurity testing and conformity assessment of IoT devices and products.
- Procedures: The CyberLAB has documented procedures for conformity assessment.
- Continued competence: Once accredited and recognized, CyberLABs would be periodically audited and reviewed to ensure they continue to comply with the IoT security standards and testing procedures.[229]

67. We adopt our proposal to accept CyberLABs, in-house labs, and CLA-run labs, to test and assess IoT products for compliance with the consumer IoT standards that are established pursuant to the process described above to actualize the outcome of the NIST criteria. Rather than having the Commission or CLA evaluate or accredit a lab, however, we are persuaded that it is appropriate to recognize testing labs that have been accredited to ISO/IEC 17025 standards to conduct compliance testing that would support an application for authority to affix the FCC IoT Label.[230] Consistent with standard practice for accreditation, the organization accrediting the testing labs must be recognized by the Bureau to perform such accreditation based on International Standard ISO/IEC 17011.[231] We recognize that labs cannot be accredited or recognized in the context of this IoT Labeling Program until after the IoT cybersecurity standards have been approved by the Commission and incorporated into the Commission's rules. We delegate authority to PSHSB to publish a Public Notice, subject to any required notice and comment, outlining the specific standards CyberLABs, in-house labs, and CLA-run labs must meet to be recognized as qualified to conduct conformity testing to support applications seeking authority to use the FCC IoT Label. We also find it to be in the public interest for the Lead Administrator to review and recognize labs that meet these accreditation requirements and make a list of recognized labs publicly available. [232]

[226] *Id.* at 11-12, para. 25.

[227] *Id.*

[228] *Id.* at 12, para. 26.

[229] *Id.*

[230] *See, e.g.,* AHAM Comments at 3; CSA Comments at 5-6; CTA Comments at 16-18; CTIA Comments at 26-27; Cybersecurity Coalition Comments at 5; ITI Comments at 8; and Widelity Comments at 3. We note that our rules will incorporate certain standards by reference, and we delegate authority to PSHSB to take any additional steps necessary, including non-substantive edits to the rule text, to effectuate the incorporation by reference.

[231] ISO/IEC 17011:2017.

[232] To enable the Lead Administrator to compile a reliable and verifiable list, we require accredited CyberLABs to submit certain information to the Lead Administrator: (1) Laboratory name, location of test site(s), mailing address and contact information; (2) Name of accrediting organization; (3) Scope of laboratory accreditation; (4) Date of expiration of accreditation; (5) Designation number; (6) FCC Registration Number (FRN); (7) A statement as to

(continued….)

68. We agree with CTIA that entities specializing in testing and certification will be valuable to program participants, and that such entities are likely to have the resources and expertise to evaluate IoT products in accordance with a standard.[233] CTIA also notes, "a third-party certification model will help to lend credibility to the program" because CyberLABs can focus on the assessment aspects of the program in a way that helps ensure the integrity of the IoT Labeling Program.[234] We also agree with CTA that leveraging accredited industry bodies to perform conformity assessments will "speed the establishment of the program and increase the program's ultimate quality."[235]

69. We agree with CSA's argument that the Commission should adopt a model where CyberLABs must be ISO/IEC 17025 accredited.[236] CSA notes its confusion as to whether CyberLABs were intended to be "certification bodies" as defined by ISO/IEC 17065 or "evaluation laboratories" as defined by ISO/IEC 17025.[237] We clarify that the proposal as envisioned by the *IoT Labeling NPRM* and adopted here is for CyberLABs, in-house labs, and CLA-run labs to function as a body responsible for assessing the security of IoT products[238] (i.e., testing lab). CSA proposes that such bodies hold ISO/IEC 17025 accreditations, as this model has been the basis for mutual recognition agreements in the cybersecurity industry,[239] and we agree.

70. We note the objection of LG Electronics, which asserts that "[t]he CyberLAB concept described in the NPRM would almost certainly create a testing bottleneck" that would slow the process, and deter participation in the IoT Labeling Program.[240] Instead, LG Electronics argues, self-certification is required to avoid these problems, although LG Electronics concedes that some compliance certification is required to participate in the IoT Labeling Program.[241] As a nascent program, and as discussed above in connection with the envisioned process, we do not find it appropriate to adopt at this time a labeling path that does not include some level of laboratory testing in combination with an application to a CLA to ensure the product bearing the FCC IoT Label complies with the IoT Labeling Program's requirements. However, we recognize the benefits of time, efficiency and cost-savings associated with in-house testing and will allow the option for applicants to use an in-house testing labs, provided the lab is ISO/IEC 17025 accredited.

71. *CyberLABs' Programmatic Role.* CyberLABs will receive requests for conformance testing from manufacturers seeking to use the FCC IoT Label and will assess and test the products using the cybersecurity standards developed by industry and approved by the Commission and provide the applicant with a report of their findings. There was confusion in the record with how the term CyberLAB

whether or not the laboratory performs testing on a contract basis; (8) For laboratories outside the United States, details of the arrangement under which the accreditation of the laboratory is recognized; and (9) Other information as requested by the Commission.

[233] CTIA Comments at 26.

[234] *Id.* at 27.

[235] *Id.* at 18.

[236] CSA Comment at 7.

[237] *Id.* at 6-7.

[238] *See IoT Labeling NPRM* at 11-12, para. 25.

[239] CSA Comments at 7.

[240] LG Electronics Comments at 2.

[241] *Id.* ("Self-certification would help avoid these problems without compromising program integrity."); *see also* Cybersecurity Coalition Comments at 6 ("The Coalition is concerned that the structure envisioned in [the *IoT labeling NPRM*] will be complex, costly, and introduce bottlenecks into the label approval process.").

is to be applied.[242] The Commission clarifies that the CyberLABs are laboratories whose role is limited to conducting compliance tests and generating reports. CyberLABs are not, in the organizational structure adopted today, either certifying products or issuing authorization to use the FCC IoT Label. While the *IoT Labeling NPRM* defined a CyberLAB as an "authorization body" we remove that reference here as the term "authorization body" might be seen as referring to certification bodies, not laboratories. The role of CyberLABs is to conduct the required tests and generate test reports for use by the applicant in seeking CLA authorization to use the FCC IoT Label.

72. *In-House Testing Lab*. We also adopt an option for manufacturers to use an accredited and Lead Administrator-recognized in-house testing lab to perform the cybersecurity conformity testing for their IoT products, provided the in-house lab meets the same vigorous standards as the CyberLABs. In the *IoT Labeling NPRM*, the Commission sought comment on whether there is an avenue for "a comprehensive review that an IoT device or product compl[ies] with the IoT security standards."[243] We received significant support in the record for an in-house testing option. Samsung argues that, to encourage widespread adoption, the Commission must allow manufacturers an option to perform in-house testing to receive the label.[244] The Cybersecurity Coalition urges the Commission to allow for in-house testing.[245] We agree that an in-house testing option, for some manufacturers, will be more cost-effective, encourage participation in the IoT Labeling Program, and when combined with the filing of an application with a CLA can assure quality and trust in the IoT Labeling Program.[246] However, we do require that in-house labs meet the same accreditation and recognition requirements as CyberLABs. In this respect, consumers may be assured that the label achieved on an in-house basis meets the same standards as those tested elsewhere, promoting consistency and reliance on the IoT Labeling Program generally. We also expect that ensuring a common baseline testing standard will ultimately aid in the ability to gain international recognition of the Cyber Trust Mark.

73. *CLA-Run Testing Lab*. We also recognize that CLAs may also have, or seek to have, their own in-house labs conduct conformity testing for applicants seeking certification to use the Mark. The Commission finds no need to limit the number of potential testing facilities by prohibiting CLA-run labs from also being considered recognized labs. Applicants who wish to do so, may file an application with an authorized CLA and request the services of the CLA's accredited and Lead Administrator-recognized lab. Again, the Commission requires CLA labs to meet the same accreditation and recognition requirements as CyberLABs. Only after a lab has been accredited by a recognized accreditation body may the lab file an application with the Lead Administrator seeking to be recognized as an approved cybersecurity testing lab. [247] As explained by A2LA, "[a]ccreditation is a means of determining the technical competence of conformity assessment organizations such as laboratories using

[242] CSA Comments at 6 ("[CSA] believes that using the new term "CyberLAB" will generate confusion. Because "CyberLAB" includes "LAB" in the name, Alliance members who read the FCC NPRM thought that the CyberLAB was an ISO 17025 organization (an "Evaluation Laboratory"). After carefully reviewing paragraph 25, it seems clear that "CyberLABs" are intended to operate as Certification Bodies, as described in ISO 17065.).

[243] *IoT Labeling NPRM* at 15, para. 32.

[244] Samsung Comments at 5.

[245] Cybersecurity Coalition at 6.

[246] *See* CSA Comments at 7-8.

[247] This approach necessitates a mechanism for the Commission to recognize lab accreditation bodies, and we accordingly adopt a rule doing so. *See infra* Appx. A, 47 CFR § 8.217. We model our approach on analogous elements of our equipment authorization rules, with which the Commission and industry have substantial experience, and which have proven workable in practice. *See* 47 CFR § 2.949. We delegate to PSHSB and OMD authority to take any necessary steps, including adoption of additional procedures and any applicable fees (pursuant to any required public notice and comment), as necessary to ensure compliance with the Communications Act with respect to any rules adopted here that contemplate the filing of applications directly with the Commission. 47 U.S.C § 158(c).

qualified, third-party accreditation bodies. It assures federal government agencies as well as private sector organizations that assessments conducted by accreditation bodies are objective and reliable and that one can have confidence in the data generated by the accredited testing laboratory."[248] Recognizing that, whether an IoT product is evaluated by a CyberLAB, CLA-run lab, or an in-house lab there is a need to ensure equal rigor in the process, this requirement applies to in-house testing labs and third party testing labs (CyberLABs and CLA-run labs). For ease of understanding, when we refer to CyberLABs below, we are including CyberLABs, in-house testing labs, and CLA-run labs.

74. In order to achieve recognition by the Lead Administrator, all labs seeking recognition under the Commission's IoT Labeling Program must submit evidence of accreditation in the form of an attestation from an accreditation body that the prospective lab has demonstrated:

1. Technical expertise in cybersecurity testing and conformity assessment of IoT devices and products. Compliance with all requirements associated with ISO/IEC 17025. If we determine that other ISO standards or other relevant requirements are missing, the Commission will provide guidance to industry on how they may be addressed.
2. Knowledge of FCC rules and procedures associated with IoT cybersecurity compliance testing and certification.
3. Necessary equipment, facilities, and personnel to conduct cybersecurity testing and conformity assessment of IoT devices and products.
4. Documented procedures for IoT cybersecurity conformity assessment.
5. Demonstrated implementation of controls to eliminate actual or potential conflicts of interests (including both personal and organizational), particularly with regard to commercially sensitive information.
6. That the applicant is not owned or controlled by or affiliated with any entity that produces equipment on the FCC Covered List or is otherwise prohibited from participating in the IoT Labeling Program. We will dismiss all applications from a company named on the Department of Commerce's Entity List, the Department of Defense's List of Chinese Military Companies.
7. That the applicant is not owned or controlled by or affiliated with any person or entity that has been suspended or debarred from receiving federal procurements or financial awards, to include all entities and individuals published as ineligible for award on the General Service Administration's System for Award Management.

75. Once accredited and recognized, the lab will be periodically audited and reviewed by the Lead Administrator to ensure they continue to comply with the IoT security standards and testing procedures.

76. Concerning items #6 and #7, national security considerations must be considered when allowing testing labs to participate because of "the unique nature of the proposed labeling program."[249] As recommended in the record and consistent with our exclusions as to eligible products and eligibility to serve as a third party administrator, all entities owned or controlled by or affiliated with entities that produce equipment found on the Covered List, as well as entities specified on the other U.S. government exclusionary lists referenced above are prohibited from serving as a CyberLAB.[250] Each of these lists represent the determination of relevant Federal agencies that the entities on the list may pose a national security threat within their respective areas, and as such we find that we cannot give U.S. Government endorsement to their security testing while claiming they pose such a threat. Insofar as the label reflects the FCC's signal to consumers about cybersecurity, it is reasonable for the FCC to take a cautious

[248] A2LA Comments at 4.

[249] CTIA Comments at 41.

[250] CTIA Reply at 7.

approach especially for those products for which relevant Federal agencies have expressed other security concerns with the testing lab.

77. NCTA also suggests also suggests that "any 'foreign entity of concern' as defined by the CHIPS Act should be ineligible for certification or recognition as a CyberLAB."[251] Further, ioXt Alliance recommends that the Commission "establish rules to ensure CyberLABs are not subject to undue influence by foreign adversaries."[252] We agree that it would be problematic for the U.S. to rely on the determination of entities controlled or affiliated with "foreign adversaries" as to the security of products approved to use the Cyber Trust Mark, and therefore the Lead Administrator will not recognize for purposes of the IoT Labeling Program any testing lab that is an entity, its affiliate, or subsidiary owned or controlled by a "foreign adversary" country. A "foreign adversary" country is defined in the Department of Commerce's rule, 15 CFR § 7.4,[253] and includes China (including Hong Kong), Cuba, Iran, North Korea, Russia, and Maduro Regime. Because of the role CLAs will play in the labeling program, we find that the concerns related to entities identified as "foreign adversaries" are equally applicable to entities acting as CLAs as they are testing labs.[254] To avoid these issues, the record suggests requiring testing labs certify compliance with the Commission's rules, including the rules pertaining to the Covered List.[255] Accordingly, we find it appropriate that each testing lab must certify to the truth and accuracy of all information included in its recognition application and immediately update the information if the information changes.

78. We also note that Garmin advocates even stricter measures on the testing labs, suggesting that the labs be "located in the U.S."[256] We decline to require physical location within the U.S. to avoid "unnecessarily limiting the pool of legitimate CyberLABs approved to conduct testing and conformity assessment for the Mark."[257] Further, the record indicates that this stricter approach "would vastly diminish manufacturers' abilities to select and access evaluation labs, conduct proper risk management and promote competition and diversity in the lab market."[258] Such a restriction might also unduly limit the ability of legitimate foreign corporations that do not raise national security concerns to participate in the IoT Labeling Program to the detriment of the goal of elevating the cybersecurity posture of those IoT devices sold in the U.S. and to promote international recognition of the Cyber Trust Mark. We delegate authority to the Bureau to adopt any additional criteria or procedures necessary with respect to labs located outside of the United States.

79. Terminating CyberLAB Testing Authority. To address national security concerns, the CyberLAB recognition afforded to entities under this IoT Labeling Program will be automatically terminated for entities that subsequently become affiliated with an entity that is owned or controlled by or

[251] NCTA Comments at 8.

[252] ioXt Alliance Reply at 6.

[253] 15 CFR § 7.4 (stating "[t]he Secretary has determined that the following foreign governments or foreign non-government persons have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons and, therefore, constitute foreign adversaries solely for the purposes of the Executive Order, this rule, and any subsequent rule" promulgated pursuant to the Executive Order); *see* 15 CFR § 7.2 ("Foreign adversary means any foreign government or foreign non-government person determined by the Secretary to have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons."); *see* Executive Order 13873 of May 15, 2019, Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 22689 (May 15, 2019).

[254] *See supra* para. 76.

[255] NCTA Comments at 8.

[256] Garmin Comments at 15.

[257] ioXt Alliance Reply at 6.

[258] CTA Comments at 27.

affiliated with entities that produce equipment placed on the Covered List, or that are otherwise added to any exclusionary list identified in this item as precluding authorization as a CyberLAB. CyberLAB testing authority may also be terminated for failure to uphold the required competencies or accreditations enumerated above. We delegate authority to the Bureau to determine when a CyberLAB's authority is to be terminated, and to terminate such authorization.[259] The Bureau may identify such deficiencies itself or receive notice from other entities, including other agencies, consumers, and industry, that products tested by a CyberLAB do not accurately reflect the security posture of the product. Products authorized to use the FCC IoT Label by a disqualified CyberLAB will be subject to the disqualification procedures described further below.

80. *Fees.* To fulfill their role, as envisioned by the *IoT Labeling NPRM*,[260] we authorize CyberLABs to charge reasonable fees to conduct the tasks adopted today. The *IoT Labeling NPRM* proposed a fee calculation methodology adopted by the Commission in the *2020 Application Fee Report and Order* and sought comment on whether any oversight is needed by the Commission over such charges.[261] We did not receive any comments on the suitability of the approach proposed in the *IoT Labeling NPRM* or detailed comments about the degree of oversight the Commission should conduct over the charges. We recognize the Cybersecurity Coalition's comments that high fees would deter participation in the IoT Labeling Program.[262] We anticipate that there will be multiple CyberLABs authorized through the approach adopted today, and we believe that market competition will ensure fees are reasonable, competitive, and accessible while covering the costs incurred by the CyberLABs in performing their designated tasks. We believe this addresses the concerns raised by the Cybersecurity Coalition and renders the approach proposed in the *IoT Labeling NPRM* unnecessary. The National Association of Manufacturers rightly indicates, however, that the fee structure for CyberLABs will necessitate "robust protections to ensure that CyberLABs focus on the underlying mission of protecting the public rather than boosting their revenues."[263] We delegate to the Bureau, in connection with OMD, to review and reconsider if necessary whether the level and structure of the fees should be regulated by the Commission.

E. Two-Step Process for Obtaining Authority to Use the FCC IoT Label

81. The Commission adopts a two-step process for a manufacturer seeking authority to use the FCC IoT Label, which includes (1) product testing by an accredited and Lead Administrator-recognized lab (e.g., CyberLAB, CLA lab, or an in-house lab) and (2) product label certification by a CLA. In the *IoT Labeling NPRM*, the Commission sought comment on the different processes that may be taken to assess conformity of consumer IoT products and devices to the Commission's IoT labeling

[259] Because of the public safety importance of a CyberLAB having the requisite qualifications and adhering to our rules when evaluating requests to use the FCC IoT Label, this process should proceed appropriately expeditiously to minimize any periods of time where a CyberLAB continues to operate in that capacity once concerns have come to PSHSB's attention. In particular, PSHSB shall provide notice to the CyberLAB that the Bureau proposes to terminate the CyberLAB's authority and provide the CyberLAB a reasonable opportunity to respond (not more than 20 days) before reaching a decision on possible termination. PSHSB may suspend the CLA's ability conduct product testing during the pendency of such consideration if appropriate.

[260] *IoT Labeling NPRM* at 20, para. 50. ("We anticipate that . . . third parties in this program may wish to charge for their services[.]).

[261] *See id.*; *Amendment of the Schedule of Application Fees Set Forth in Sections 1.1102 through 1.1109 of the Commission's Rules*, MD Docket No. 20-270, Report and Order, 35 FCC Rcd 15089, 15127, para. 115-117 (2020). Application fees are adjusted every two years to reflect changes in the Consumer Price Index. *See, e.g., Amendment of the Schedule of Application Fees Set Forth in Sections 1.1102 through 1.1109 of the Commission's Rules*, MD Docket No. 20-270, Order, FCC 22-94 (2023).

[262] Cybersecurity Coalition Comments at 14.

[263] NAM Comments at 4.

rules.[264] The *IoT Labeling NPRM* noted that the Commission's equipment authorization program, as currently administered, only allows for two authorization procedures: (1) Certification (which requires the filing of an application) and (2) Supplier's Declaration of Conformity (SDoC).[265] In the context of this IoT Labeling Program and as discussed in detail below, we find that in order to ensure the integrity of this nascent program, that the FCC IoT Label certification process will include a two-step process involving (1) the use of an accredited and Lead Administrator-recognized laboratory (CyberLAB, CLA lab, or in-house lab) to test the IoT product for compliance to FCC rules and generate a test report; and (2) an application to an FCC-recognized CLA (i.e., an accredited certification body) to certify the product as fully compliant with all relevant FCC IoT Labeling Program rules.

1. Product Testing by an Accredited and Recognized Lab

82. The record is split on the processes the Commission should adopt for manufacturers to follow when seeking to use the FCC IoT Label, specifically with regard to whether it is necessary for a third party to review and verify the product meets all of the IoT Labeling Program requirements, including product testing, or if the manufacturer should be afforded the opportunity to "self-declare" compliance and affix the FCC IoT Label without third party verification.[266]

83. UL Solutions, TÜV SÜD, and TIC Council Americas recommend that the Commission require all applications to be supported by conformity testing conducted by an accredited lab (e.g., ISO/IEC 17025 accredited),[267] and submitted to a third party for verification of compliance with the Commission's program requirements. [268] Others argue the Commission should accept a declaration of

[264] *IoT Labeling NPRM* at 15, para. 32; *see also* ISO/IEC 17000:2004, Conformity assessment - Vocabulary and general principles, defines conformity assessment as "demonstration that specified requirements relating to a product, process, system, person or body are fulfilled." Conformity assessment includes sampling and testing, inspection, supplier's declaration of conformity, certification, and management system assessment and registration. It also includes accreditation of the competence of those activities by a third party and recognition (usually by a government agency) of an accreditation program's capability. ANSI, National Conformity Assessment Principles for the United States (2007), https://share.ansi.org/Shared%20Documents/News%20and%20Publications/Brochures/NCAP%20second%20edition.pdf [https://perma.cc/2H5E-VSDH].

[265] The *IoT Labeling NPRM* used the SDoC process, self-attestation and self-certification interchangeably. However, we clarify that the inclusion of these new terms was not an indication of change of policy or regulations to equipment authorization rules or any FCC rules.

[266] As explained by A2LA, "[a] common practice in conformity assessment is self-declaration. This is when organizations test and inspect their own products and declare that they meet a standard. Caution needs to be practiced due to the bias inherent in self-declaration. Accreditation is a means of determining the technical competence of conformity assessment organizations such as laboratories using qualified, third-party accreditation bodies. It assures federal government agencies as well as private sector organizations that assessments conducted by accreditation bodies are objective and reliable and that one can have confidence in the data generated by the accredited testing laboratory." A2LA Comments at 4.

[267] UL Solutions Comments at 2 (supporting conformity testing by an in-house lab, but only where the testing is aligned to ISO 17025 requirements, which will "enable a standardized approach and level playing field."); TÜV SÜD Comments at 3 (opposing allowing manufacturers to perform self-assessments in their internal labs because the results are not independent); TIC Council Americas Comments at 6 ("[Due to the] higher level of risk associated with the cybersecurity of IoT products, the complex technical nature of the testing, and the need for consistent and impartial adherence to the standards for the fidelity of the label and the benefit of the consumer—testing for the authorization of the use of the label should only be performed by those with the recognized competency to do so. Self-assessment by manufacturers to the program's standards should be permitted only where the manufacturer laboratory has met this bar, such as accreditation to ISO/IEC 17025.").

[268] UL Solutions Comments at 5-6 (explaining that given the high-threat environment in which IoT devices operate and the potential for digital and physical harms that can result from a cyberattack, requiring assessment by an independent third party before a product bears the Cyber Trust Mark "best serves consumers and best enables the development of a consistent, effective, trustworthy program.").

conformity or self-certification,[269] while others recommend the Commission enter into agreements with each manufacturer to allow the manufacturer to conduct internal conformity testing of its products and self-certify compliance with the Commission's program requirements resulting in approval to use the Cyber Trust Mark without third party involvement.[270] CTA, for example, contemplates a "Manufacturer Self-Attestation Process" where manufacturers apply to the Commission for access to a "Mark Self-Attestation License Agreement" between the manufacturer and the FCC. Under this process, the manufacturer provides documentation showing how it complies with the NIST Criteria and if the Commission agrees with the documentation, the parties execute the agreement. The license agreement will identify the limits of the manufacturer's license authority, which may be corporate-wide, on a divisional basis, or for a specific product line.[271]

84. To ensure the Cyber Trust Mark retains the highest level of integrity and consumer trust, we agree with commenters who caution against allowing testing by entities that are not accredited and recognized. We also agree with Garmin and AHAM, who recommend third party verification of the information contained in a manufacturer's application to use the Cyber Trust Mark.[272] UL Solutions notes that while the Commission's equipment authorization process allows some products that pose a low risk of RF interference to be approved via an SDoC, there is no clear line to be drawn between low risk and high risk connected products when "IoT devices are significant targets for an ever- growing number of cybersecurity attacks."[273] In addition, UL Solutions points to the investigation conducted by the Government Accountability Office (GAO) into the ENERGY STAR program's initial reliance a supplier's declaration of conformity, which GAO found to be unreliable because GAO was able to obtain UL certification with blatantly non-conforming products.[274]

85. The Commission disagrees with commenters who believe the IoT Labeling Program should offer different methods of conformity assessment based on varying levels of risk and potential impact on consumers because doing so adds an unnecessary and significant layer of complexity to the

[269] Keysight Comments at 2; NAM Comments at 4; Samsung Comments at 5; NCTA Comments at 8-9 (suggesting "[c]onformity assessment by accredited third-party labs is an effective means to ensure that the Program reflects high cybersecurity standards," but if the Commission determines self-certification should be permitted, the self-certification should match the same administrative requirements and level of testing vigor offered by a CyberLAB and not afford manufacturers a way to bypass program requirements); CSA Comments at 12 (arguing that self-attestation or SDoC is critical to the success of the program, and manufacturers should be transparent about their results and applications should be reviewed by an ISO 17025 accredited entity for completeness and consistency with the Labeling Program requirements, but the "review should not involve re-testing the device as that would defeat the purpose of the self-attestation option–to reduce the cost and delay to market for innovative new products.").

[270] Garmin Comments at 5; CTA Comments at 24 ("The program should prioritize self-assessment and self-approval processes as the structure underlying a self-attestation option to use the Mark.").

[271] CTA Reply Comments at Annex, A-14 to A-15.

[272] *See* Garmin Comments at 13; *see also* AHAM Comments at 3 (arguing manufacturers should be permitted to conduct the required testing and provide a test report to a third party certifier who reviews the test report and decides whether to adopt the results and certify that the product meets the Commission's program requirements and manufacturers should be able to be qualified as CyberLABs).

[273] UL Solutions Comments at 5 (citing e.g., David Paul, *IoT Devices See More Than 1.5bn Cyberattacks so Far This Year* (Sept. 13, 2021), https://www.digit.fyi/iot-security-kaspersky-research-attacks/ [https://perma.cc/B7E5-35BF]; James Coker, *Smart home experiences over 12,000 cyber-attacks in a week* (July 2, 2021), https://www.infosecurity-magazine.com/news/smart-home-experiences-cyber/ [https://perma.cc/D6L6-2GLH]; Jill McKeon, *IoT Malware Attack Volume up 123% in Healthcare* (July 28, 2022), https://healthitsecurity.com/news/iot-malware-attack-volume-up-123-in-healthcare).

[274] UL Solutions Comments at 5 (citing Government Accountability Office, Energy Star Program, Covert Testing Shows the Energy Star Program Certification Process Is Vulnerable to Fraud and Abuse, GAO-10-470 (2010), https://www.gao.gov/assets/files.gao.gov/assets/gao-10-470.pdf [https://perma.cc/9VB5-ZWTA] (GAO Report)).

process. The Commission recognizes the view of Keysight, NEMA, AIM, Whirlpool, AHAM, Consumer Reports, Garmin, NAM, ITI, and TIC Council Americas, who support self-attestation as an efficient and cost effective methodology for applicants to conduct conformity assessments.[275] However, the Commission agrees with A2LA, which urges caution with self-attestations of conformity "due to the bias inherent in self-declaration."[276] We also take into serious consideration the 2010 GAO Report that found the ENERGY STAR program in effect at that time, which was "primarily a self-certification program relying on corporate honesty and industry self-policing to protect the integrity of the Energy Star label,"[277] failed to require upfront third party validation of manufacturers' self-reported claims of compliance with the program requirements, which resulted in the certification of bogus products as ENERGY STAR compliant.[278] ENERGY STAR has since changed the manner in which it certifies products as ENERGY STAR compliant, stating that in order "[t]o ensure consumer confidence in the ENERGY STAR label and to protect the investment of ENERGY STAR partners, the U.S. Environmental Protection Agency (EPA) requires all ENERGY STAR products to be third-party certified. Products are tested in an EPA-recognized laboratory and reviewed by an EPA-recognized certification body before they can carry the label."[279]

86. As such, in light of the nascent nature of the IoT Labeling Program, lessons learned in the ENERGY STAR context, and the need to ensure that the Cyber Trust Mark garners sufficient trust by consumers to be viewed as providing accurate information and manufacturer participation, we find that allowing a path to "self-attestation" is not appropriate at this time. While such a path may provide for prompt time to market for the Cyber Trust Mark itself, the concerns regarding the Mark's integrity at this initial stage counsel against "self attestation." Moreover, we anticipate that the benefits and level of efficiency afforded manufacturers by the ability to use in-house labs will mitigate the additional process associated with certification by a CLA, as discussed below.

2. Filing an Application with a CLA

87. We intend for the Cyber Trust Mark to serve as a reliable and trusted way for consumers to quickly identify those products that meet the Commission's program requirements. To achieve this, the Commission must adopt sufficient controls over the IoT Labeling Program to ensure only those products that meet the Commission's requirements bear the Cyber Trust Mark. The Commission's second step of requiring an application be submitted to a CLA is a significant and important control to ensure that an independent disinterested third party outside the manufacturer's control has reviewed the manufacturer's product application and supporting test report and verified that the product complies with the Commission's program requirements.

88. The second step of the application process is particularly important because, as discussed above, the Commission allows the first step (testing) to be completed by an accredited and recognized CyberLAB, a CLA lab, or the manufacturer's in-house lab. Requiring the manufacturer to submit an application with a CLA is an important control, particularly to ensure that all products, including those products whose conformity testing is conducted, and reports are generated, by the manufacturer's in-

[275] *See* Coalition Letter Reply at 2; Keysight Comments at 2; NEMA Comments at 5; AIM Comments at 3; Whirlpool Comments at 4 (supports self-attestation especially for lower risk IoT, but notes self-attestation should be validated by a third party to protect the integrity of the program); AHAM Comments at 3; Samsung Comments at 5; Consumer Reports Comments at 20; Garmin Comments at 12; NAM Comments at 4; ITI Reply at 4; TIC Council Americas Reply at 1.

[276] A2LA Comments at 4; *see also* Ravnitzky Comments at 1.

[277] GAO Report at 8.

[278] GAO Report at 7.

[279] ENERGY STAR, *Third-Party Certification*, https://www.energystar.gov/partner_resources/products_partner_resources/third_party_cert [https://perma.cc/N6HG-JRKW] (last visited Jan. 16, 2024).

house lab, are subject to third party scrutiny and oversight. As such, the Commission requires all entities seeking to use the FCC IoT Label must submit an application for authority to a CLA to use the FCC IoT Label that is supported by the appropriate report detailing the conformity testing conducted by a lab that is both accredited and Lead Administrator-recognized (CyberLAB, CLA lab, or manufacturer's in-house lab). Only entities who have received prior authorization from a CLA (i.e., cybersecurity certification) are authorized to use the FCC IoT Label, which will ensure the IoT Labeling Program retains its integrity.[280] We further recognize that the CLA may charge a reasonable fee to cover the cost of reviewing the application and the costs of conducting the other tasks the CLA would perform. Once the IoT Labeling Program is established, we may revisit the issue of whether to adopt additional pathways to obtaining authority to use the FCC IoT Label.

89. The *IoT Labeling NPRM* sought comment on whether and how one or more third party administrators should be utilized to manage the IoT Labeling Program, and whether the Commission should designate one or more administrators to authorize use of the label.[281] Kaiser Permanente argues that the Commission should maintain ownership of the application process, as well as oversight and supervision of third parties administering the IoT Labeling Program.[282] Garmin notes that the application process described in the *IoT Labeling NPRM* is unclear and worries that third party involvement would require enormous effort, and cautioned that sharing sensitive information with a third party administrator itself raises security concerns.[283] However, the record was silent with respect to details about an application process. We agree that oversight and supervision of the IoT Labeling Program, including intaking applications, will require effort but believe a CLA is in the best position to streamline that process and, as noted, ensure the integrity of the process. We will require the CLA to have the ability to securely handle large volumes of information, which we believe should alleviate Garmin's concern.[284] We outline the application process to use the FCC IoT Label below.

90. Before being able to display the Cyber Trust Mark, the applicant must determine their product is an eligible product under our rules; have their product tested by an accredited and Lead Administrator-recognized CyberLAB, CLA Lab, or manufacturer's in-house lab; obtain a report of conformity and compliance from the lab; and submit an application for authority to use the FCC IoT Label to an FCC-recognized CLA in accordance with their procedures. Using the CLAs' filing processes, entities seeking authority to use the FCC IoT Label will file an application to be developed by the Bureau. Each application must include a report of conformity issued by an accredited CyberLAB, accredited CLA lab, or accredited in-house lab whose testing and reporting is comparative in rigor to that completed by a CyberLAB. The CLA will review the application and supporting documentation to ensure it is complete and in compliance with the Commission's rules and will either grant or deny the application. If an application is granted, the CLA will provide the applicant with notification of the grant and authority to affix the FCC IoT Label to the product granted authorization.

91. Applications that do not meet the Commission's IoT Labeling Program will be denied by the CLA. If an application is denied, the CLA will provide the applicant with notification of the denial and an explanation of why it was denied. An applicant may only re-submit an application for a denied product if the CLA-identified deficiencies have been corrected. The applicant must indicate on its

[280] In addition to the discussion in the text, we adopt certain rules to support the administration and integrity of the IoT Labeling Program, including governing the designation of agents for service of process and governing required signatures. *See infra*, Appx. A, 47 CFR § 8.207(b)(5), (d). We model our approach on analogous elements of our equipment authorization rules, with which the Commission and industry have substantial experience, and which have proven workable in practice. *See* 47 CFR § 2.911(d)(7), (f).

[281] *IoT Labeling NPRM* at 11, para. 23.

[282] Kaiser Permanente Comments at 3.

[283] Garmin Comments at 12.

[284] *See supra* para. 59 (requiring CLAs to "[demonstrate] ability to securely handle large volumes of information and demonstration of internal security practices.").

application that it is re-submitting the application after it was denied, the name of the CLA that denied the application, and the CLA's explanation of why it was denied. Failure to disclose the denial of an application for the same or substantially similar product will result in denial of the application for that product and the FCC will take other regulatory and/or legal action it deems appropriate.

92. Grant or denial of an application for authority to use the FCC IoT Label will be made by the CLA in the first instance. The CLA will return incomplete applications to the applicant or otherwise contact the applicant regarding the incomplete application, as soon as possible.

93. We delegate authority to the Bureau to issue a Public Notice after any necessary notice and public comment and after completing any process required under the Paperwork Reduction Act, providing further details on how to apply for authority to use the FCC IoT Label, including but not limited to informational elements of the application, additional details on filing requirements (e.g., description or photograph of the label and how/where it will be affixed to the product), and how to request confidential treatment of submitted information. As the Commission anticipated in the NPRM,[285] CLAs may charge reasonable fees for their services and to cover the costs of performing the administrative duties. The *IoT Labeling NPRM* proposed to follow the fee calculation methodology adopted by the Commission in the *2020 Application Fee Report and Order* and requested comment on the proposal and any changes.[286] We did not receive any comments on the suitability of this approach. We recognize the Cybersecurity Coalition's comments that high fees would deter participation in the IoT Labeling Program.[287] We anticipate that there will be multiple administrators authorized through the approach adopted today, and we believe that market competition will ensure fees are reasonable, competitive, and accessible while covering the costs incurred by the CLA in performing their designated tasks. We believe this addresses the concerns raised by the Cybersecurity Coalition and renders the approach proposed in the *IoT Labeling NPRM* unnecessary. We therefore reject the NPRM's proposal. To the extent that the Lead Administrator may incur costs in performing its duties on behalf of the program as a whole, we expect these costs to be shared among CLAs as a whole.[288] We delegate to the Bureau, in connection with OMD, to consider these issues and provide guidance to the CLAs and Lead Administrator to ensure the fees do not become onerous, as indicated by the record.[289]

94. *Seeking Review of CLA Decision.* Any party aggrieved by an action taken by a CLA must first seek review from the CLA, which must be filed with the CLA within 60 days from the date of the CLA's decision. A party aggrieved by an action taken by a CLA may, after seeking review by the CLA, seek review from the Commission. A request for Commission review must be filed with the Commission within 60 days from the date the CLA issues a decision on the party's request for review. In all cases of requests for review, the request for review shall be deemed filed on the postmark date. If the postmark date cannot be determined, the applicant must file a sworn affidavit stating the date that the request for review was mailed. Parties must adhere to the time periods for filing oppositions and replies set forth in 47 CFR § 1.45.

[285] *IoT Labeling NPRM* at 20, para. 50.

[286] *Amendment of the Schedule of Application Fees Set Forth in Sections 1.1102 through 1.1109 of the Commission's Rules*, MD Docket No. 20-270, Report and Order, 35 FCC Rcd 15089, 15127, para. 115-117 (2020). Application fees are adjusted every two years to reflect changes in the Consumer Price Index. *See, e.g., Amendment of the Schedule of Application Fees Set Forth in Sections 1.1102 through 1.1109 of the Commission's Rules*, MD Docket No. 20-270, Order, FCC 22-94 (2023).

[287] Cybersecurity Coalition Comments at 14.

[288] *See supra* para. 52 (describing the duties of the Lead Administrator). We recognize that many of the duties of the Lead Administrator benefit all the CLAs and the program as a whole, and we do not suggest that the costs associated with the duties of the Lead Administrator as described in this Order to be an exhaustive list of the shared costs we expect to be shared among CLAs as a whole.

[289] *See* Cybersecurity Coalition Comments at 14.

95. We delegate authority to PSHSB to consider and act upon requests for review of CLA decisions. Requests for review that raise novel questions of fact, law, or policy will be considered by the full Commission. An affected party may seek review of a decision issued under delegated authority pursuant to the rules set forth in part 1 of the Commission's rules. The Bureau will conduct de novo review of requests for review of decisions issued by a CLA. The Commission will conduct de novo review of requests for review of decisions by the CLA that involve novel questions of fact, law, or policy; provided, however, that the Commission will not conduct de novo review of decisions issued by the Bureau under delegated authority. The Bureau will, within 90 days, take action in response to a request for review of CLA decision that is properly before it. The Bureau may extend the time period for taking action on a request for review of a CLA decision for a period of up to 90 days. The Commission may also at any time, extend the time period for taking action of a request for review of a CLA decision pending before the Bureau. The Commission will issue a written decision in response to a request for review of a CLA decision that involves novel questions of fact, law, or policy within 90 days. The Commission may extend the time period for taking action on the request for review of a CLA decision. The Bureau also may extend action on a request for review of an CLA decision for a period of up to ninety days. While a party seeks review of a CLA decision, they are not authorized to use the FCC IoT Label until the Commission issues a final decision authorizing their use of the FCC IoT Label.

F. Consumer IoT Product Cybersecurity Criteria and Standards

96. *Technical Criteria for Consumer IoT Products*. In the *IoT Labeling NPRM*, the Commission sought comment on adopting NIST's recommended IoT criteria (NIST Core Baseline), which are discussed in detail in NISTIR 8425, as the basis for the IoT Labeling Program.[290] The Commission also asked whether there are other IoT criteria it should consider and whether there are separate criteria that should be considered for higher risk IoT devices or classes of devices.[291] We adopt the *IoT Labeling NPRM* proposal that the NIST Core Baseline serve as the basis of the IoT Labeling Program. The NIST Core Baseline is based on product-focused cybersecurity capabilities (also referred to by NIST as "Outcomes") rather than specific requirements, which NIST asserts provide the flexibility needed due to the diverse marketplace of IoT products, and we agree. As outlined in the IoT Labeling *NPRM*, the NIST criteria includes the following IoT product capabilities: (1) asset identification; (2) product configuration; (3) data protection; (4) interface access control; (5) software update; (6) cybersecurity state awareness; and the following IoT Product Developer Activities: (7) documentation; (8) information and query reception; (9) information dissemination; and (10) product education and awareness.[292]

97. The record reflects broad support for adoption of the technical criteria presented in NISTIR 8425. For example, a coalition of industry stakeholders including the Association of Home Appliance Manufacturers, Connectivity Standards Alliance, Consumer Technology Association, CTIA Information Technology, Industry Council, National Electrical Manufacturers Association, Plumbing Manufacturers International Power Tool Institute, Security Industry Association, Telecommunications Industry Association, U.S. Chamber of Commerce, and USTelecom submitted a letter to the Commission supporting the establishment of "a voluntary program based on the technical criteria developed by

[290] *IoT Labeling NPRM* at 13, para. 27 (citing Appendix A (describing the NIST criteria)); *see also* NISTIR 8425.

[291] *Id.*

[292] NISTIR 8425 at 4; *NIST Cybersecurity White Paper* at 4-10 (Feb. 4, 2022); NIST, *Report for the Assistant to the President for National Security Affairs (APNSA) on Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software, A summary review of labeling actions called for by Executive Order (EO) 14028: Improving the Nation's Cybersecurity* at 4 (2022), https://www.nist.gov/system/files/documents/2022/05/24/Cybersecurity%20Labeling%20for%20Consumers%20under%20Executive%20Order%2014028%20on%20Improving%20the%20Nation%27s%20Cybersecurity%20Report%20%28FINAL%29.pdf [https://perma.cc/PA4J-DD76] (*NIST Summary Report*).

[NIST], under NISTIR 8425."[293] UL Solutions supports adoption of the NISTIR 8425 criteria and asserts that there are several mature standards that can be drawn from that address the NISTIR 8425 criteria, such as UL 2900, UL 5500, and IEC 62443.[294]

98. CTIA supports adoption of the NIST Core Baseline, but urges the Commission not to prescribe any specific methodologies that testing programs or standards must use, other than to require that such programs or standards be consistent with NIST Core Baseline.[295] CSA also supports adoption of the NIST Core Baseline, but urges the Commission to refrain from developing its own standards for testing.[296] Rather, CSA asserts that they have developed a certification program that meets the requirements of NISTIR 8425 and other relevant standards documents, including ETSI EN 303 645 and the Singapore Cybersecurity Labeling Scheme,[297] and CTA indicates that they are working on American National Standards (ANS) documents that will "[d]efine a Framework that is a standardized and objective method of applying the Criteria in NISTIR 8425 to a candidate Scheme or to a manufacturer's proposal for self-attestation…"[298] Garmin encourages the Commission to consider ETSI 303 645 standards,[299] and commenters American Certification Body, Inc. and Consumer Reports encourage international standards such as those developed as a result of the EU Cyber Resiliency Act and UK's Product Security and Telecommunications Infrastructure Act.[300] These commenters did not oppose referencing the NIST criteria.

99. We agree with Infineon, Consumer Reports, and NCTA and adopt NISTIR 8425 as the basis for the Commission's IoT Labeling Program.[301] The consumer IoT environment is complicated by a significant number of different types of consumer IoT products. Adoption of the NIST criteria as the foundation of the IoT Labeling Program will result in a robust consumer IoT program that is sufficiently flexible that it can be applied across all types of consumer IoT products. The NIST criteria were developed through a multi-year effort between NIST and various stakeholders, and includes significant industry input and will continue to be updated by NIST as necessary. The Commission agrees with NIST's publication, which avers that the following NISTIR 8425 criteria identify the cybersecurity capabilities that consumers would expect manufacturers to address within the products they buy. NIST

[293] Coalition Letter Reply at 1. *See also*, CSA Comments at 8-9 ("[CSA] recommends prompt adoption of NISTIR 8425 as the basis for the program"); CTIA Comments at 16; CTA Comments at 11; NCTA Comments at 5; Consumer Reports Comments at 16-17; ioXt Alliance Comments at 6; Cybersecurity Coalition Comments at 7; UL Solutions Comments at 4; ITI Comments at 7; TechNet Comments at 2; Comcast Comments at 11; Kaiser Permanente Comments at 3; NTCA Reply at 3; AHAM Comments at 4; Samsung Comments at 3; NYC Cyber Command Office of Technology & Innovation Comments at 3 (supporting consideration of the Cloud Security Alliance's IoT Framework, based on sourced NIST controls) (NYC OTI).

[294] *See, e.g.*, UL Solutions Comments at 4.

[295] *See* CTIA Comments at 22.

[296] CSA Comments at 10-11.

[297] *Id.*

[298] CTA Reply at A-1; *see also* CTIA *Ex Parte*.

[299] *See* Garmin Comments at 10.

[300] *See* American Certification Body, Inc. Reply at 1 (encouraging incorporation of international standards such as the EU Cyber Resiliency Act); Consumer Reports Comments at 18-19 (recommending the UK's Product Security and Telecommunications Infrastructure Act).

[301] *See, e.g.*, Infineon Comments at 2 ("Infineon recommends that the Commission adhere as closely as possible to NISTIR 8425, which is one of the best and most widely recognized cybersecurity standards for IoT."); Consumer Reports Comments at 18 (The NIST 8425 document creates an excellent starting place for setting the criteria for a certification program and should be used to develop the framework."); NCTA Comments as 5-6 ("Building the Program on the foundation of [NISTIR 8425]'s already-established process and guidance would maintain a consistent federal approach to IoT security baseline requirements[.]").

contemplates that most of the criteria concern the IoT product directly and are expected to be satisfied by software and/or hardware implemented in the IoT product (1-6 below) and other criteria apply to the IoT product developer (7-10 below).[302] The following is the list of the NIST IoT product capability criteria, NIST's brief description of each, and the NIST-identified cybersecurity utility for each:[303]

(1) Asset Identification: The product can be uniquely identified by the customer and other authorized entities and the product uniquely identifies each IoT product component and maintains an up to date inventory of connected product components

   i. Cybersecurity Utility: The ability to identify IoT products and their components is necessary to support such activities as asset management for updates, data protection, and digital forensics capabilities for incident response.

(2) Product Configuration: The configuration of the IoT product is changeable, with an ability to restore a secure default setting, and changes can only be performed by authorized individuals, services, and other IoT product components.

   i. Cybersecurity Utility: The ability to change aspects of how the IoT product functions can help customers tailor the IoT product's functionality to their needs and goals. Customers can configure their IoT products to avoid specific threats and risk they know about based on their risk appetite.

(3) Data Protection: The IoT product protects data store across all IoT product components and transmitted both between IoT product components and outside the IoT product from unauthorized access, disclosure, and modification.

   i. Cybersecurity Utility: Maintaining confidentiality, integrity, and availability of data is foundational to cybersecurity for IoT products. Customers will expect that data are protected and that protection of data helps to ensure safe and intended functionality of the IoT product.

(4) Interface Access Control: The IoT product restricts logical access to local and network interfaces – and to protocols and services used by those interfaces – to only authorized individuals, services, and IoT product components.

   i. Cybersecurity Utility: Enumerating and controlling access to all internal and external interfaces to the IoT product will help preserve the confidentiality, integrity, and availability of the IoT product, its components, and data by helping prevent unauthorized access and modification.

(5) Software Update: The software of all IoT product components can be updated by authorized individuals, services, and other IoT product components only by using a secure and configurable mechanism, as appropriate for each IoT product component.

   i. Cybersecurity Utility: Software may have vulnerabilities discovered after the IoT product has been deployed; software update capabilities can help ensure secure delivery of security patches.

(6) Cybersecurity State Awareness: The IoT product supports detection of cybersecurity incidents affecting or affected by IoT product components and the data they store and transmit.

   i. Cybersecurity Utility: Protection of data and ensuring proper functionality can be supported by the ability to alert the customer when the device starts

[302] NISTIR 8425 at 2; *NIST Cybersecurity White Paper* at 4-10; *NIST Summary Report* at 4.

[303] NISTIR 8425 at 5-10; *see also IoT Labeling NPRM* at Appendix A.

operating in unexpected ways, which could mean that unauthorized access is being attempted, malware has been loaded, botnets have been created, device software errors have happened, or other types of actions have occurred that was not initiated by the IoT product user or intended by the developer.

The following is the list of NIST-identified IoT Product Developer Activities/Non-Technical Supporting Capabilities and their NIST-identified cybersecurity utility:[304]

(7) Documentation: The IoT product developer creates, gathers, and stores information relevant to cybersecurity of the IoT product and its product components prior to customer purchase, and throughout the development of a product and its subsequent lifecycle.

   i. Cybersecurity Utility: Generating, capturing, and storing important information about the IoT product and its development (e.g., assessment of the IoT product and development practices used to create and maintain it) can help inform the IoT product developer about the product's actual cybersecurity posture.

(8) Information and Query Reception: The IoT product developer has the ability to receive information relevant to cybersecurity and respond to queries from the customer and others about information relevant to cybersecurity.

   i. Cybersecurity Utility: As IoT products are used by customers, those customers may have questions or reports of issues that can help improve the cybersecurity of the IoT product over time.

(9) Information Dissemination: The IoT product developer broadcasts (e.g., to the public) and distributes (e.g., to the customer or others in the IoT product ecosystem) information relevant to cybersecurity.

   i. Cybersecurity Utility: As the IoT product, its components, threats, and mitigations change, customers will need to be informed about how to securely use the IoT product.

(10) Product Education and Awareness: The IoT product developer creates awareness of and educates customers and others in the IoT product ecosystem about cybersecurity-related information (e.g., considerations, features) related to the IoT product and its product components.

   i. Cybersecurity Utility: Customers will need to be informed about how to securely use the device to lead to the best cybersecurity outcomes for the customers and the consumer IoT product marketplace.

100. *Consumer IoT Product Standards*. The *IoT Labeling NPRM* recognized that the Commission's "conformity assessment program must be based on IoT security standards and testing requirements that the IoT devices and products must satisfy to be eligible to receive and use the label."[305] The *IoT Labeling NPRM* proposed that standards be developed jointly with industry and other stakeholders and asked for comments on who should convene these stakeholders and develop standards that allow for "the consistent and replicable testing necessary to ensure the outcome based NIST IoT labeling criteria are fulfilled."[306] The Commission sought comment on whether the Commission or an outside entity is in the best position to convene these stakeholders. The *IoT Labeling NPRM* also sought comment on the relevant industry consensus standards that may already exist and should be considered by

[304] NISTIR 8425 at 11-16.

[305] *IoT Labeling NPRM* at 13, para. 28.

[306] *Id*.

the Commission for the IoT Labeling Program, or whether new standards need to be developed.

101. We find that standards are necessary to administer the IoT Labeling Program in a fair and equitable manner and to ensure the products with the FCC IoT Label have all been tested to the same standards to provide consumers with confidence that products bearing the FCC IoT Label include strong cybersecurity. Commenters generally agree with the adoption of standards based on NIST's Core Baseline for Consumer IoT products (NISTIR 8425).[307] We take up the Cybersecurity Coalition's recommendation "that the Commission or a designated third-party administrator work with stakeholders to identify recognized standards that encompass the Core Baseline, or that offer equivalent controls."[308] NCTA also notes that "Standards Development Organizations ("SDOs") and specification organizations are well-established organizations that can develop standards aligned with NIST guidelines and the Program's goals."[309] According to NIST, the NISTIR 8425 "*outcomes* are guidelines that describe **what** is expected… but more specific information may be needed to define how to implement IoT products or product components so that they meet an outcome. *Requirements* define **how** a component can meet an outcome for a specific use case, context, technology, IoT product component etc. …."[310]

102. We reject CTIA's recommendation that the Commission refrain from adopting specific standards and solely rely on the NIST criteria.[311] Rather, the Commission agrees with NIST and commenters that its criteria are general guidelines that must be further developed into a requirements document (i.e. standards) and corresponding testing procedures, which will demonstrate how the product bearing the FCC IoT Label has met the NIST criteria and to ensure consistency of application across a class of products. ITI adds that the "Commission need not recreate [existing] work or develop its own standards but can leverage completed standards work for swift development and implementation."[312] The integrity of the Cyber Trust Mark requires the Commission to adopt standards that provide for adequate and consistent testing of products to ensure that all products bearing the FCC IoT Label have demonstrated conformance to the identified standards that the Commission has approved as compliant with the NIST criteria. In addition, for the Commission's IoT Labeling Program to be fairly administered by the multiple CLAs, all products displaying the FCC's label must be tested against the same standards to ensure that all products displaying the FCC IoT Label conform to the Commission's standards.

103. Commenters such as TÜV SÜD agree that "the main requirement when perform[ing] testing for compliance is that the test need[s] to be reliable and always offer the same outcome when a product is tested in the same condition. In the current state of the NIST IoT criteria there is not enough detail[] in the standard, so there is the need to write a more detail[ed] test method/standard."[313] UL Solutions also "supports the use of the NISTIR 8425 criteria as the basis for the IoT Labeling Program. These criteria help establish a minimum security baseline suitable for consumer IoT products… However, as noted in paragraphs 27 and 28 [of the *IoT Labeling NPRM*], these criteria must be defined by minimum IoT security requirements and standards to enable consistent and replicable product testing."[314] Moreover, Somos similarly agrees that leveraging existing standards for device definition and security guidelines are the fastest, most effective path to the definition of a secure ecosystem, that NIST 8425 standard is the appropriate starting point, and that "existing standards should allow for the Commission to

[307] *See, e.g.*, Cybersecurity Coalition Comments at 6; UL Solutions Comments at 4; Samsung Comments at 3.

[308] Cybersecurity Coalition Comments at 6-7.

[309] NCTA Comments at 6.

[310] IoT Product Component Requirements Essay at 1-2 (emphasis in original).

[311] CTIA Comments at 16.

[312] ITI Reply at 5.

[313] TÜV SÜD Comments at 3.

[314] UL Solutions Comments at 4.

quickly create its definitions and guidelines."[315] We agree with the Cybersecurity Coalition that "only those standards and best practices recognized by the labeling program should be eligible, in order to avoid the inclusion of non-credible or irrelevant frameworks that may undermine trust in the label."[316]

104. We further determine that, given the existing work in this space, the Commission should not undertake the initial development of the standards that underpin the NIST Core Baseline. Rather, as discussed in paragraph 56 above, we direct the Lead Administrator to undertake this task, and delegate authority to the Bureau to review and approve the consumer IoT cybersecurity standards and testing procedures that have been identified and/or developed by the Lead Administrator (after any appropriate public comment) that ensures the product to which a manufacturer seeks to affix the FCC IoT Label conforms to the NIST criteria. NIST's *IoT Product Component Requirements Essay* provides a summary of standards and guidance that NIST has initially identified as applicable to IoT devices and IoT product components, that the Lead Administrator may determine are applicable to the IoT Labeling Program.[317] Moreover, the Lead Administrator may also determine existing standards or schemes that exist in the market already may be readily adaptable and leverage such work to meet the terms of the program.

105. The Commission recognizes that since a "product" for purposes of the IoT Labeling Program is comprised of at least one IoT device and any additional product components that are necessary to use the IoT device beyond basic operational features, there may be multiple standards (e.g., a package of standards) applicable to a single IoT product (e.g., standards applicable to IoT devices; mobile apps; networking equipment included with IoT devices; and cloud platforms). The Commission does not anticipate a single standard would be developed or identified to apply to *all* consumer IoT products. However, a single package of standards may be developed or identified for each product type or class as identified by the Lead Administrator and reviewed and approved by the Bureau. We also agree with the Cybersecurity Coalition that "participants should have discretion to include security features that go beyond standard requirements . . . So long as the additional security features do not conflict with conformity with the standard used for eligibility by the labeling program participants, participants should be encouraged to go beyond baseline requirements."[318]

G. The FCC IoT Label (Cyber Trust Mark and QR Code)

106. We adopt the *IoT Labeling NPRM's* proposal to implement a single binary label with layering.[319] As discussed in the *IoT Labeling NPRM*, "under a binary label construct, products will either qualify to carry the label or not qualify (i.e., not be able to carry the label) and 'layers' of the label would include the Commission's Cyber Trust Mark representing that the product or device has met the Commission's baseline consumer IoT cybersecurity standards and a scannable code (e.g., QR Code) directing the consumer to more detailed information of the particular IoT product."[320]

107. We adopt a binary label because we believe that a label signaling that an IoT product has met the minimum cybersecurity requirements will be simplest for consumers to understand, especially as the label is introduced to and established for the public. The Cybersecurity Coalition supports a binary label, citing the benefits of a simple, consumer friendly nature and its potential to streamline the purchasing decision for consumers.[321] Similarly, as LG points out, "[l]ike the ENERGY STAR program,

[315] Somos Reply at 1.

[316] Cybersecurity Coalition Comments at 6-7.

[317] IoT Product Component Requirements Essay at 3-7.

[318] Cybersecurity Coalition Comments at 6-7.

[319] *IoT Labeling NPRM* at 16, para. 35.

[320] *Id.* (internal footnotes omitted).

[321] Cybersecurity Coalition Comments at 1; *see also, e.g.*, CTA Comments at 32 ("CTA supports the Commission's proposal, consistent with NISTIR 8425, to implement a single, binary label with layered information. This approach

(continued….)

a binary label specifying that a device has met a government standard – in this case for cybersecurity – will be enough to drive consumers and manufacturers toward more secure products," while leaving manufacturers free to separately provide additional cybersecurity information about their products.[322] And the Connectivity Standards Alliance supports the use of a single binary label with layering, as recommended by NIST, asserting that "[a]cademic studies have validated this approach."[323] Conversely, Canada advocates a multi-tiered approach to labeling to "lower barriers to entry into the labelling regime and facilitate trade and competition by ensuring Micro, Small and Medium Sized Enterprises (MSMEs), with fewer resources to meet a high level of cybersecurity," and to "provide the incentives for a greater number of firms to innovate in IoT products and work on 'climbing the ladder' of cybersecurity levels over time."[324] Another commenter suggests a multi-tiered label that would have different colors depending on the length of time the product is supported.[325] Other commenters advocate a multi-tiered approach that need not be reflected in different Cyber Trust Marks, but in different information available when a consumer scans the QR code.[326] A study by Carnegie Mellon University indicates that different types of labels of various complexities have varying levels of effectiveness, but does not contest the idea of a binary label.[327] We also recognize that some international regimes, such as Singapore, use a multi-tiered label.[328]

108. Although one could imagine myriad different approaches to labeling that each have relative advantages and disadvantages, on balance we are persuaded to rely on a binary label as we begin our IoT Labeling Program, consistent with NIST's recommended approach. We agree with the Cybersecurity Coalition that "the primary value of the IoT . . . labeling program is to better enable ordinary consumers to distinguish labeled products as likely providing better basic security than unlabeled products."[329] We believe a binary label meets this goal by providing a clear indication that products with the label meet the Commission's cybersecurity requirements. We anticipate that promoting early consumer recognition of the FCC IoT Label—which we think is better advanced by a binary label—will, in turn, make consumers more attuned to cybersecurity issues and more receptive to additional cybersecurity information that manufacturers elect to provide apart from the FCC IoT Label and associated QR code. Thus, we believe that our use of a binary label still retains incentives for manufacturers to innovate and achieve higher levels of cybersecurity. Our approach to determining what cybersecurity standards will be applied also accommodates the potential for different requirements being

will allow consumers to rapidly assess product security at point-of-sale and provide more detailed, up-to-date information to consumers or subject matter experts conducting a more thorough review of a product's capabilities." (footnote omitted)).

[322] LG Electronics Comments at 2.

[323] Connectivity Standards Alliance Comments at 13.

[324] Government of Canada Comments at 1.

[325] Jason Cole Comments at 1.

[326] *See, e.g.*, CTIA Comments at 28.

[327] *See* Carnegie Mellon and Duke Researcher Comments at 5.

[328] Cyber Security Agency of Singapore, *Cybersecurity Labeling Scheme (CLS) for Consumers*, https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/for-consumers [https://perma.cc/X3MG-MKZ4] (last visited Jan. 8, 2024); *see also, e.g.*, Government of Canada Comments at 1 (noting Singapore's program and advocating "instituting a number of levels of cybersecurity that firms could choose to meet"); People's Republic of China Comments at 4-5 (advocating "that the U.S. utilize the internationally recognized IoT product network security level classification system to further specify the safety level standards for related products in this [labeling] program, and provide specific requirements for classification certification and corresponding label information based on the level").

[329] Cybersecurity Coalition Comments at 1.

necessary to meet the NIST baseline criteria in different contexts.[330] To the extent that any multi-tiered labeling approach contemplated by commenters would allow manufacturers to obtain a label through lesser cybersecurity showings, that would be less effective at achieving the goals of our program. And to the extent that any multi-tiered labeling approach would require manufacturers to make heightened cybersecurity showings to achieve higher-tier labels, that is unlikely to lower barriers to participation in the IoT Labeling Program while also risking less understanding and acceptance of the FCC IoT Label by consumers. Because delay in moving forward with the IoT Labeling Program would have its own costs in pushing back the potential for benefits to consumers and device security, we also recognize the benefits of a binary label as more straightforward to implement, at least at the start of our IoT Labeling Program. Weighing all the relevant considerations, we are persuaded to move forward with a binary label at this time.

109. We require that products bearing the FCC IoT Label, which includes the Cyber Trust Mark, must also include the corresponding QR Code. Approval to use the Cyber Trust Mark is conditioned on the label also bearing the QR Code in accordance with the IoT Labeling Program's label standards. In addition, the FCC IoT Label must be easily visible to consumers (e.g., on product packaging). This approach received considerable support in the record. We agree with USTelecom that "consumers should not have to open the package to get information because that could impact their ability to return the product."[331] Power Tool Institute, Inc. concurs that "[p]lacing a QR Code on the packaging is preferable to placing it on the device."[332] Notable pros of using a QR Code are providing "consumers with detailed information about a device or product,"[333] enhancing the program's objective by providing real-time updates.[334] However, some commenters raise concerns with the placement of the QR Code on the product packaging. Logitech urges the Commission to not require a QR Code in conjunction with the label, stating that it could crowd packaging, cause consumer confusion, and may cause confusion if retailers scan the wrong barcode when checking out a customer.[335] We believe that as the label becomes established and recognized by consumers and retailers, the benefit of providing a QR Code linking to a registry populated with current information on the IoT product outweighs the potential for consumer confusion. We also believe the registry will be of value to consumers such that they will want to see it acknowledged in an easily accessible manner, which will override any potential difficulty retailers may have with scanning the incorrect code. Moreover, recognizing the realities of inventory turnover against the need for a cybersecurity label to be dynamic, the use of a QR Code-embedded URL in this context ensures that (1) if a consumer desires more information about the product than what the label itself signifies there is a simple means of access; and (2) information associated with the product's compliance with the IoT Labeling Program is current. We view these as relevant considerations to purchasing decisions, which requires easy access to such information "on the spot" rather than requiring a purchaser to independently seek it out.

110. We direct the Lead Administrator to collaborate with stakeholders as needed to recommend to the Commission standards for how the FCC IoT Label bearing the Cyber Trust Mark and the QR Code should be designed (e.g., size and white spaces) and where such a label should be placed. This should include where the label could be placed on products where consumers may not see product packaging when shopping or after purchasing (e.g., refrigerators, washing machines, dryers, dishwashers, etc.) and including where consumers purchase products online. In addition, the Lead Administrator

[330] *See supra* paras. 56-58.

[331] USTelecom Comments at 8.

[332] Power Tool Institute Comments at 3 (PTI).

[333] Kaiser Permanente Comments at 4.

[334] NYC OTI Comments at 4.

[335] Logitech Comments at 3.

should address the use of the FCC IoT Label in store displays and advertising.[336] We recognize the current work being done by industry on an appropriate format for the label, including the Cybersecurity Label Design, which is part of CTA's ANSI-accredited standards program.[337] As noted by CTA in its reply comments, the FCC specifies requirements for the use of the Cyber Trust Mark, but "there are several additional details needed regarding QR coding and resolution, white space for accurate recognition of QR codes, and more."[338] CTA states that the draft ANSI/CTA-2120 details lay out requirements for packaging, and we encourage the Lead Administrator to review and consider the work CTA's Cybersecurity Label Design working group (a subgroup of CTA's Cybersecurity and Privacy Management Committee) has completed in this regard.[339] We agree that we should take into consideration the considerable work that has already been undertaken with respect to labeling design and placement and seek to leverage and benefit from this expertise by directing the Lead Administrator to seek feedback from a cross-section of relevant stakeholders who have been working on these issues. We delegate authority to PSHSB to review, approve (or not approve) the Lead Administrator-recommended labeling design and placement standards after any required public notice and comment process and if approved incorporate into the Commission's Part 8 rules. The provisions of 47 CFR § 2.935(a) (allowing the electronic display of "or other information that the Commission's rules would otherwise require to be shown on a physical label attached to the device" do not apply to the FCC IoT Label. [340] The Cyber Trust

[336] The issue of where the FCC IoT Label would be placed was raised in the record. We agree that flexibility in placement is important in instances where the consumer might not see the product's packaging, such as in larger appliances, before purchasing the product. *See* AHAM Comments at 5; NAM Comments at 5. We recognize that some types of products might be customarily displayed in ways that make a one-size-fits-all approach inappropriate. As such, we agree with the ioXt Alliance's suggestion that we consider how the label may be placed in ways that will be helpful to a consumer, such as through an in-store display, advertisement on a screen, or website. *See* ioXt Alliance Comments at 20.

[337] CTA Reply at A-7.

[338] *Id.* at A-8.

[339] *Id.* at A-7 to A-9.

[340] By their term, those rules – which allow certain electronic labeling of "information that the Commission's rules would otherwise *require* to be shown on a physical label" – do not apply to a voluntary program that permits the use of the FCC IoT Label for entities meeting the relevant criteria of that voluntary program. 47 CFR § 2.935(a) (emphasis added); *see also, e.g.*, *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, 8758, para. 28 (2017) (explaining that the proposed rules "generally would allow a radiofrequency device to electronically display any labels *required* by our rules, including the FCC ID required for certified devices, as well as any warning statements or other information that our rules require to be placed on a physical label on the device" (emphasis added)); *id*. at 8763-64, para. 41 (discussing the rules' application "[i]f the Commission imposes (under current or future regulations) a *requirement* that a device physically bear a label with regulatory information"). The regulatory context also supports that understanding. The E-LABEL Act, which the Commission was implementing when adopting the relevant rules, likewise appears focused on the general sorts of mandatory labeling requirements the Commission had in place in 2014. *See, e.g.*, E-LABEL Act, Pub. L. No. 113-197, § 2(1) (2014) (discussing "physical label requirements" of the sort established by the Commission in 1974 and refined over time); *id*., § 3 (adopting provisions codified at 47 U.S.C. § 622(a) defining "electronic labeling" as "displaying required labeling and regulatory information" and focusing on equipment and devices "required under regulations of the Commission to be authorized by the Commission before the equipment or device may be marketed or sold within the United States"). Independently, the Commission's focus on the types of mandatory label or information disclosure requirements of the sort imposed under its equipment authorization rules when adopting section 2.935 of the rules persuades us that those e-labeling rules should not apply to the IoT Labeling Program at this time, given our conscious decision to make the program "new and distinct," consistent with commenters' urging to keep the equipment authorization and IoT Labeling programs separate. *See supra* para. 43; *see also* 47 U.S.C. § 302a(a) (authorizing the Commission to adopt "reasonable regulations" based on its assessment of "the public interest, convenience, and necessity); *id*., § 622(b) (directing the Commission to take "appropriate" action "as necessary" with respect to e-labeling).

Mark may only be used as directed by Part 8, notwithstanding 47 CFR § 2.935 or any other rule.

H. Registry

111. We adopt our proposal from the *IoT Labeling NPRM* that the label include the Cyber Trust Mark and a QR Code that links to a decentralized publicly available registry containing information supplied by entities authorized to use the FCC IoT Label (e.g., manufacturers) through a common Application Programming Interface (API). The registry will include and display consumer-friendly information about the security of the product. We believe a publicly accessible registry furthers the Commission's mission of allowing consumers to understand the cybersecurity capabilities of the IoT devices they purchase. We also agree that it is important for the registry to be dynamic, so a consumer can be aware if a product loses authorization to use the FCC IoT Label or if the manufacturer is no longer providing security updates.[341] There is robust support for the development of a publicly-accessible registry.[342] We agree with NCTA that "the IoT Registry is foundational to the value and utility of the Cyber Trust Mark Program."[343] In the following paragraphs, we establish general parameters for registry information.

112. In the *IoT Labeling NPRM*, the Commission proposed a single registry associated with the IoT Labeling Program and that the QR Code included as part of the FCC IoT Label include a link to the information about the product on the registry webpage.[344] Today, we adopt a decentralized registry that contains specific essential information that will be disclosed by the manufacturer, as discussed in further detail below. This essential information from the manufacturer will be provided to a consumer accessible application via the registry by utilizing a common API. When a consumer scans the QR Code, a consumer accessible application will access the registry using the common API and present the consumer with the information we require to be displayed from the registry. CTIA points out that a centralized registry containing all the information the Commission conceived in the *IoT Labeling NPRM* and by commenters in the record would be inordinately complex and costly.[345] We agree, and endeavor to meet the policy goal of providing a transparent, accessible registry to the public through more efficient and less complicated means.

113. We agree with the Commission's assessment in the *IoT Labeling NPRM* that the registry's goal is to assist the public in understanding security-related information about the products that bear the Cyber trust Mark.[346] CTIA confirms this view, stating "the Commission should focus on the [registry] as a means to provide consumers with information that is critical to the success of the program."[347] CTIA further proposes that we should allow each manufacturer to establish their own mechanisms for conveying this information to consumers.[348] However, we acknowledge ioXt's concern that a completely manufacturer-driven approach could lead to inconsistencies, inaccuracies, or other difficulties for the consumer.[349] To balance the need for a workable, streamlined registry that is consistent for consumers and meets the Commission's goals while easing the administrative burden inherent in a centralized registry, we require a common API that would provide access to the following essential

[341] Cybersecurity Coalition Comments at 11.

[342] CSA Comments at 15; NCTA Comments at 9; Infineon Comments at 2; WiFi Alliance Comments at 2; USTelecom Comments at 9; AIM Comments at 4; Planar Comments at 2.

[343] NCTA Comments at 9.

[344] *IoT Labeling NPRM* at 18, para. 41.

[345] CTIA Reply at 10-11.

[346] *See IoT Labeling NPRM* at 18, para. 41.

[347] CTIA Reply at 12.

[348] *Id.*

[349] ioXt Reply at 11.

information from the manufacture and display it to the consumer in a simple, uniform way:[350]

(1) Product Name;
(2) Manufacturer name;
(3) Date product received authorization (i.e., cybersecurity certification) to affix the label and current status of the authorization (if applicable);
(4) Name and contact information of the CLA that authorized use of the FCC IoT Label;
(5) Name of the lab that conducted the conformity testing;
(6) Instructions on how to change the default password (if the default password can be changed);
(7) Information (or link) for additional information on how to configure the device securely;
(8) Information as to whether software updates and patches are automatic and how to access security updates/patches if they are not automatic;
(9) Guaranteed minimum support period for the product (which may be zero, but must be disclosed);
(10) Disclosure of whether the manufacturer maintains a Software Bill of Materials (SBOM); and
(11) Additional data elements that the Bureau determines are necessary pursuant to the delegated authority discussed in paragraph 121 below.

114. To reduce potential burdens and focus on essential information, we pare back the scope of the registry from what the Commission proposed in the *IoT Labeling NPRM*. We agree with the Cybersecurity Coalition that "[t]he primary purpose of the label is to help consumers make informed purchasing decisions"[351] and include in the registry information that is key to making a purchasing decision, without overwhelming the consumer.[352] To this end, we agree with commenters who suggest that including the information proposed in the *IoT Labeling NPRM* may be too burdensome. NEMA, for example, expresses concern about the resources required for a registry containing a full catalogue of devices.[353] CTIA agrees that the IoT registry envisioned by the *IoT Labeling NPRM* would "impose significant, unmeetable burdens" for participants and the manager of the registry, and encourages us to refine our approach.[354] The Cybersecurity Coalition likewise expresses concern over the complexity of the proposed registry.[355] We agree that the registry be "modest in its goals" and "limited to basic information that is uniform . . . and pragmatic and useful to the consumer."[356] We believe that a registry containing simple, easy to understand information will be most helpful to a consumer making a purchasing decision. Focusing only on the most critical information will further facilitate the speedy establishment of the IoT Labeling Program and the registry itself.

[350] We note that the use of an API as part of the registry was recommended by CSA, the National Retail Foundation, and Widelity. Along with the benefits of an API that we identify here, the use of an API provides other benefits to other stakeholders in industry and retailers, while providing stakeholders with information that could assist with innovation and potential expansion of the registry to provide additional functions. *See* CSA Comments at 16; National Retail Foundation Comments at 1-2 (NRF); Widelity Comments at 3.

[351] Cybersecurity Coalition Comments at 9.

[352] CTIA Comments at 31 ("Ultimately, the Commission must ensure that information conveyed to consumers . . . strikes the right balance between giving consumers valuable information . . . and overloading consumers with information that will be difficult to maintain and update, confuse consumers, and even tip off bad actors.").

[353] NEMA Comments at 6.

[354] CTIA Comments at 29.

[355] Cybersecurity Coalition Comments at 11.

[356] CTA Reply at 13.

115. In the interest of keeping information simple and establishing the database swiftly, we streamline the elements that should be included in the registry. We do require information about how to operate the device securely, including information about how to change the password, as it would help consumers understand the cybersecurity features of the products, how those products are updated or otherwise maintained by the manufacturer, and the consumer's role in maintaining the cybersecurity of the product.[357] We do not require information about whether a product's security settings are protected against unauthorized changes as part of the initial rollout of the registry in an attempt to streamline the registry to address concerns that the registry would be too bulky or unfriendly to consumers. However, we delegate authority to the Bureau to consider whether to include this requirement at a later date, as discussed below. Nor do we require the location where the product was manufactured. As the Association of Home Appliance Manufacturers points out, the location of the product's manufacture is redundant with existing legal requirements.[358] We also do not require labels to include an expiration date at this time as it may not be an applicable requirement for every product,[359] but we agree with commenters that the registry should indicate the minimum guaranteed product support period.[360]

116. While we recognize the value of utilizing the registry to keep consumers informed about product vulnerabilities, we note CTIA and Garmin's concerns about listing unpatched vulnerabilities as not providing value to consumers, discouraging manufacturers from participating in the program, and tipping off bad actors.[361] We agree that these concerns are significant and do not require detailed information about vulnerability disclosures in the registry at this time. Rather, we require disclosure only of whether a manufacturer maintains an SBOM for supply chain security awareness. We agree with Consumer Reports, NYC Cyber Command Office of Technology and Innovation (NYC OTI), and the Cybersecurity Coalition that an SBOM should be considered as an element of the registry.[362] We also note that Garmin's concern is with disclosing the specific contents of an SBOM to the public, which "could reveal confidential business relationships with companies, as well as provide a roadmap for attackers,"[363] but this is not what we require here. Requiring participating manufacturers to disclose only the maintenance of an SBOM, rather than the contents therein, indicates an added level of software security while also protecting potentially sensitive information. Further, while we agree with CTA that a searchable registry would have value for the public,[364] we are mindful of the resources, costs, and time involved with creating a registry that is searchable by each of the elements identified in the *IoT Labeling*

[357] *See* Widelity Comments at 2 ("[A] Registry containing information on IoT . . . and their cybersecurity features . . . would allow consumers . . . to easily access information on a product's security features, vulnerabilities, and updates[.]"); *see also* Consumer Reports Reply Comments at Appendix A.

[358] AHAM Comments at 5; *see* 16 CFR § 500.5 ("The label of a consumer commodity shall specify conspicuously the name and place of business of the manufacturer, packer, or distributor.").

[359] *IoT Labeling NPRM* at 19-20, paras. 47-48; *see also infra* Section III.I (describing the record and setting forth tasks with respect to determining the renewal process).

[360] CSA Comments at 21-22; Letter from Grace Burkard, Director of Operations, ioXt Alliance, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 23-239 (Dec. 14, 2023) at 2; see also Letter from Marco Peraza, Legal Advisor, FCC, *on behalf of Hacker News Members*, to PS Docket No. 23-239 (Sept. 14, 2023) (during the Hacker News website public Q&A and discussion session commenters generally support a requirement that manufacturers be required to support their devices for a minimum period; vendors should disclose the period for which they support a device; and certain classes of devices should have a mandatory minimum support period.).

[361] CTIA Comments at 30-32; Garmin Reply at 2.

[362] Consumer Reports Comments at 3; NYC OTI Comments at 5; Cybersecurity Coalition Comments at 10-12; *see also* FDA Comments at 4 (noting that submission of a software bill of materials to the Secretary is required for FDA-regulated medical devices).

[363] Garmin Reply at 3.

[364] CTA Comments at 34.

NPRM.[365] In limiting the registry as we have, we address the concerns that the registry may be too complex to administer in the initial iteration of the IoT Labeling Program. As discussed above, the decentralized, API-driven registry we adopt today addresses the complexity concerns raised in the record. We cabin our initial vision of the registry and direct the Bureau, as described further below, to consider ways to make the initial design of the registry modest, with potential to scale the registry as the IoT Labeling Program grows.

117. In this respect, we note that NIST's research suggests that "future work should be done to examine potential issues of including an expiry date on a label."[366] NIST cited studies conducted by the UK government that consumers were confused about what the expiration date meant, and an Australian government study in which consumers thought the device would stop working after that date.[367] The UK research did conclude, however, that continued manufacturer support was important to survey participants.[368] Consumer Reports suggested an expiration date, if present, should be tied to an end-of-support date rather than a renewal date.[369] NIST's research into the importance of support dates to consumers coupled with the potential confusion of expiration dates and the support from the record lead us to conclude an expiration date is not warranted. We do find, however, that the disclosure of a minimum support period for the device is appropriate, and will provide meaningful information to consumers on the manufacturer's commitment to provide patches or other support – a vital issue in a dynamic threat environment.

118. While we identify the defined set of data that is consistent across all manufacturers, we believe the information contained in the registry for a particular IoT product or product class may also depend on the standards and testing procedures adopted for each particular IoT product. As such, in the near term, we expect there will be additional registry data elements that are specific to an IoT product, or classes of IoT products, that are not yet ripe for decision in this Order. We also recognize that some of the information recommended by NIST in its consumer education recommendations, discussed in further detail below, may be valuable for consumers to see in the registry.[370] Accordingly, while we provide a baseline of necessary information that must be displayed for an IoT product in the registry, regardless of class the IoT product belongs to, we delegate authority to the Bureau to determine, subject to any required public notice and comment processes, whether any additional disclosure fields are necessary, and if so, what they should be.

119. We disagree with commenters, such as LG, who suggest that manufacturers should have discretion over whether to include additional privacy and/or security information through a QR Code,

[365] *See* Letter from Stacey Higginbotham, Policy Fellow, Consumer Reports, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 23-239 (Dec. 13, 2023) referencing Consumer Reports, *CR Cyber Trust Mark IoT Security Registry Design Proposal* at 5, n.5 (Dec. 12, 2023) (*Consumer Reports Registry Design Proposal*) (describing a site capable of searching by product identifiers and manufacturers as "more sophisticated" and suggesting that initial design of the registry should not be overly complex).

[366] Julie M. Haney & Susanne M. Furman, *Smart Home Device Loss of Support: Consumer Perspectives and Preferences* at 503, NIST (2023), https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=936232 [https://perma.cc/EL5G-TSL5] (*NIST Consumer Perspectives Research*).

[367] *NIST Consumer Perspectives Research* at 503.

[368] *NIST Consumer Perspectives Research* at 498 (describing the importance of security updates for different types of devices, where between 77% and 90% of participants "strongly agree or agree" that security updates were important depending on the device type).

[369] Consumer Reports Comments at 33.

[370] *See infra* Section III.L.

URL, or other scannable mechanism insofar as it would require additional information in the registry.[371] LG Electronics, though supportive of adding a variety of data to the registry, acknowledges it is unclear how much detail or what types of information would be of value to a consumer.[372] We believe that allowing discretion over what information is included in the registry may overcrowd it, or engender consumer confusion. Rather, uniform registry elements will provide greater consistency for consumers and adoption of uniform registry elements is supported by the record.[373] We make clear, however, that we do not otherwise restrict what information manufacturers may include or reference on their product packaging, so long as it does not interfere with or undermine the display of the FCC IoT Label.

120. We recognize that a decentralized registry relying on data derived through an API from manufacturers will require some oversight to ensure that the registry, when accessed by consumers using QR Codes, functions as described and displays the required information about individual products. We direct the Lead Administrator to receive and address any technical issues that arise in connection with displaying the registry through the QR Code, the associated API, and consumer complaints with respect to the registry. CSA recommends that the Commission engage a third party with operating the registry for cost and efficiency reasons.[374] CTA agrees that the Commission should use a third party to host and manage the registry due to the resources required to establish the registry.[375] We agree that, given the structure of the registry as we adopt it today, the Lead Administrator is in the best position to interface with manufacturers to ensure the smooth operation of the registry.

121. We also recognize that for a registry of this magnitude to be effectively and timely rolled out requires significant input and coordination with industry partners. To determine how the registry should be structured to best meet the goals of the IoT Labeling Program as we adopt it today, we direct the Bureau to seek comment and consider, as part of a public process, the technical details involved with the operation of the registry. We delegate authority to the Bureau to adopt a Public Notice, subject to any required public notice and comment, identifying the common API; how the API should be structured; how the API should be used; how the queried data will be displayed to the consumer; how manufacturers need to maintain and implement the API in connection with its interactions with the registry; what, if any, additional disclosure fields would be most beneficial to consumers in the future, as discussed above; how the data in the registry returned by the API should be presented to the consumer; how the costs involved in maintaining the registry will be handled; how often the registry should be updated;[376] and whether data should be replicated in multiple repositories – by the relevant CLA(s) or vendors, for example – and publicly accessible via a single query point; and any other technical information needed to establish the registry as we adopt today. We delegate authority to PSHSB in coordination with, at a minimum, OMD (specifically the Office of the Chief Information Officer) and, to the extent necessary OGC (specifically the Senior Agency Official for Privacy) to identify and impose any applicable security or privacy requirements arising from Federal law or Federal guidance for the registry and to approve or modify the recommendations regarding the functional elements of the registry listed above. We further delegate

[371] *See* LG Electronics Comments at 2 ("[A]lthough LG supports the NPRM's proposal to implement a single binary label, manufacturers should have discretion over whether to provide additional security or privacy information through a QR Code, URL, or other scannable mechanism.").

[372] *Id.*

[373] Cybersecurity Coalition Comments at 9-10; Planar Comments at 2 (describing the European Product Registry for Energy Labeling as a model where "[c]overed products sold [that] bear [the label] contain[] a QR code that leads the consumer to a webpage with full details about the product's energy consumption").

[374] CSA Comments at 15-16 ("The Alliance recommends that the Commission hire a third-party administrator to operate the IoT registry because this will likely result in a more cost-effective and efficient solution[.]").

[375] CTA Comments at 38.

[376] *See, e.g.*, *Consumer Reports Summer Research* at 4 ("Consumers are interested in the security of their connected devices and the data those devices collect about them."); Consumer Reports Comments at 6 ("The FCC needs to establish a mechanism to ensure the registry stays up to date.").

authority to PSHSB to publish a Public Notice, subject to any required public notice and comment, adopting and incorporating into the Commission's rules any additional requirements or procedures necessary to implement the Cyber Trust Mark registry.

I. Continuing Obligations of Entities Authorized to Use the FCC IoT Label

122. We adopt the proposal in the *IoT Labeling NPRM* that applicants must renew their authority to use the FCC IoT Label. Entities authorized to use the FCC IoT Label are required to ensure the product bearing the FCC IoT Label continue to comply with the Commission's program requirements. We disagree with CCDS that no renewals should be required and the product should simply bear the last date of testing. Such an approach could severely impair consumer trust in the label, especially if a product bearing the FCC IoT Label is being sold as new but is far out of date as to its initial achievement of the Mark.

123. For those that support some interval of renewal, the record is divided with respect to whether IoT Labeling Program applicants should file for renewal each year, as proposed in the *IoT Labeling NPRM*.[377] Consumer Reports and TÜV SÜD agree that annual renewal is appropriate.[378] AHAM feels that an annual renewal application as the Commission proposed was unnecessary, or at minimum "unnecessarily rigid."[379] AHAM posits that a requirement to renew should only be triggered when a significant or substantive change is made to either the standard the manufacturer certifies to, or a significant design change to the product.[380] Similarly, more durable IoT products (such as smart appliances) may need to be renewed less frequently.[381] NAM argues that annual renewals are unnecessary for products that pose a limited risk.[382] Kaiser Permanente believes higher-risk devices should be updated annually, and otherwise renewal should occur every three years.[383] CCDS argues no annual testing is necessary, and the product should simply have the date it was authorized to bear the label that signals the product was compliant as of the initial date.[384] CSA suggests limiting the need for annual testing, but suggests some kind of annual reporting should be required.[385] We observe that other certifying bodies, such as ioXt, require annual renewal for products they certify and allow incentives for early renewal.[386] Based on the record, we recognize the degrees of nuance attendant to the different types of products at issue. We agree with the notion that certain IoT products, depending on their lifespan and risk level, may need different standards for renewal to achieve the FCC IoT Label.

124. We task the Lead Administrator to collaborate with stakeholders and provide recommendations to PSHSB on how often a given class of IoT products must renew their request for authority to bear the FCC IoT Label, which may be dependent on the type of product, and that such a recommendation be submitted in connection with the relevant standards recommendations for an IoT product or class of products. In doing so, consideration should be given as to whether annual continuous compliance reports are acceptable for purposes of renewing, and how to effectively balance the need for industry flexibility and the need to ensure that consumers have up-to-date information about the product they are considering purchasing. Consideration should also be given to the fees incurred as part of a

[377] *IoT Labeling NPRM* at 19, para. 47.

[378] Consumer Reports Comments at 19; TÜV SÜD Comments at 2.

[379] AHAM Comments at 4.

[380]*Id.*; Whirlpool Comments at 5; CTA Reply at 7.

[381] AHAM Comments at 4-5.

[382] NAM Comments at 5.

[383] Kaiser Permanente Comments at 2.

[384] CCDS Comments at 5.

[385] CSA Comments at 19.

[386] ioXt Comments at 23.

renewal process, as we agree with Kaiser Permanente that renewal fees must not be unduly burdensome or cost-prohibitive.[387] We emphasize that renewals should occur frequently enough that a consumer can be sure that a product bearing the FCC IoT Label has reasonable cybersecurity protections in place, and some process must be in place to ensure accountability, even if annual testing is not required. We delegate authority to PSHSB to review, approve (if appropriate) and, subject to any required public notice and comment, incorporate by reference into the Commission's rules, the proposals from the Lead Administrator for renewal of authority to bear the FCC IoT Label.

J. Audits, Post-Market Surveillance, and Enforcement

125. We adopt the *IoT Labeling NPRM*'s proposal to rely on a combination of administrative remedies and civil litigation to address non-compliance and direct the CLA(s) to conduct post-market surveillance. The *IoT Labeling NPRM* sought comment on how to enforce program requirements to ensure the integrity of the Cyber Trust Mark is maintained.[388] We asked whether non-Commission entities should conduct random audits and/or market surveillance, who those entities should be, and what audit requirements should be included.[389] We also sought comment on what enforcement measures would be appropriate to address fraudulent uses of the FCC IoT Label.[390] The purpose of this IoT Labeling Program is to provide reasonable assurances to the consumer that the products they bring into their homes have at least a minimum level of cybersecurity. The success of the IoT Labeling Program hinges on the label retaining its integrity as a trusted consumer resource. This requires vigorous review and enforcement to ensure that products bearing the Cyber Trust Mark are in compliance with the program standards. We further observe that the ISO/IEC 17065 standards require CLAs to perform appropriate post-market surveillance activities. We adopt post-market surveillance and civil enforcement, accordingly.

126. We find support in the record that the "Mark must be trusted by consumers to be successful"[391] and "to gain consumer confidence and incentivize cybersecurity, the label must be backed by a robust enforcement program."[392] We agree with the EPIC's position that weak enforcement may result in unmet consumer expectations regarding a product's actual level of cybersecurity and "allow bad actors to take advantage of the goodwill created by the cybersecurity program,"[393] and take up its recommendation of independent, post-market audits accordingly.[394] Whirlpool also supports regular market surveillance to find instances of unapproved use of the Cyber Trust Mark, as well as products that may have been certified but no longer meet program requirements.[395] Whirlpool states that surveillance "should include random auditing… as well as sampling of some established percentage on a regular basis of certified products/devices."[396] The American Association for Laboratory Accreditation supports adopting the product surveillance standards established for TCBs and in the EPA's ENERGY STAR

[387] Kaiser Permanente Comments at 5.

[388] *IoT Labeling NPRM* at 20-21, para. 51.

[389] *Id.*

[390] *Id.*

[391] Whirlpool Comments at 6.

[392] EPIC Reply at 26.

[393] *Id.* at 27.

[394] *Id.* at 27-31.

[395] *See* Whirlpool Comments at 6.

[396] *Id.*

program.[397] We also agree with commenters who indicate that the Commission, CLAs, and possibly the Federal Trade Commission (FTC) should be able to receive complaints of noncompliant displays of the Cyber Trust Mark, which could result in auditing.[398] We delegate authority to the Bureau, in coordination with the Consumer and Governmental Affairs Bureau, to determine the process for receiving and responding to complaints. CTA and Planar Systems also support random auditing.[399] We agree that random audits, in addition to regular post-market surveillance will best serve to maintain consumer confidence in the Cyber Trust Mark. [400]

127. *Post-market surveillance*. We agree with the Cybersecurity Coalition that post-market surveillance of products receiving the Cyber Trust Mark should be a principal enforcement mechanism,[401] and find that CLAs are in the best position to conduct post-market surveillance and random auditing, in accordance with ISO/IEC 17065. These activities are based on type testing a certain number of samples of the total number of product types which the CLA has certified. In addition, each CLA must be prepared to receive and address post-market surveillance from the public. If a CLA determines that a product fails to comply with the technical regulations for that product, the CLA will immediately notify the grantee and the Lead Administrator in writing. The grantee will have 20 days to provide a report to the CLA describing actions taken to correct the deficiencies. Continued deficiency after 20 days will result in termination of the grantee's approval to display the Cyber Trust Mark. A grantee's approval to display the Cyber Trust Mark may also be terminated subject to the 20 day cure period for false statements or representations found in their application or associated materials or if other conditions come to the attention of a CLA which would warrant initial refusal to authorize use of the FCC Label. Such terminations will protect the integrity of the FCC IoT Label and encourage accurate representations and disclosures in application materials that will enhance the reliability of the Labeling Program's operation, more generally. We delegate authority to the Bureau to develop procedures that CLAs will use for performing post-market surveillance, including specific requirements such as the number and types of samples that a CLA must test and the requirement that grantees submit, upon request by PSHSB or a CLA, a sample directly to the CLA to be evaluated for compliance at random or as needed.[402] We also delegate authority to the Bureau to establish requirements (subject to any required public notice and comment) regarding post-market surveillance of products in any instances where the CLA that granted the authorization of the product is not available to conduct such post-market surveillance. The document will also address procedures to be followed if a grantee's approval to display the Cyber Trust Mark is terminated based on mandatory post-market surveillance or notice from the public, including

[397] A2LA Comments at 2; *see also* OET Knowledge Database, *TCB Post-Market Surveillance* (Apr. 26, 2022), https://apps.fcc.gov/kdb/GetAttachment.html?id=dQfN6tcMcj%2FrEmjHGZ%2B3dw%3D%3D&desc=610077%20D01%20TCB%20Post%20Market%20Surveillance%20v06r02&tracking_number=20540 [https://perma.cc/FA7K-ZXSR] (outlining post-market surveillance responsibilities of TCBs) (*TCB Post-Market Surveillance*).

[398] *See* Cybersecurity Coalition Comments at 14; EPIC Reply at 33.

[399] CTA Comments at 25; Planar Comments at 2.

[400] To enable a meaningful audit process it will be important to be able to review certain key records, which we consequently will require grantees to retain records regarding the original design and specifications and all changes that have been made to the relevant consumer IoT product that may affect compliance with the IoT Labeling Program requirements; a record of the procedures used for production inspection and testing; and a record of the test results that demonstrate compliance. *See infra* Appx. A, 47 CFR § 8.214. We model our approach on analogous elements of our equipment authorization rules, with which the Commission and industry have substantial experience, and which have proven workable in practice. *See* 47 CFR § 2.938(a), (f).

[401] Cybersecurity Coalition Comments at 14; *see also* Ricardiam DAO LLC Comments at 1 (listing regular periodic security audits as a key component for the program).

[402] If necessary to accommodate the volume of auditing, a CLA may outsource some post-market surveillance testing to a recognized CyberLAB, but retains responsibility for the final review. *See e.g.*, *TCB Post-Market Surveillance*, Section E(2) at 3 (describing a similar process for outsourcing post-market testing for the Equipment Authorization program).

disqualification from the IoT Labeling Program and potential further investigation into other products related to the manufacturer or the CyberLAB, as discussed below. Finally, the Lead Administrator will submit periodic reports to PSHSB of the CLAs' post-market surveillance activities and findings in the format and by the date specified by PSHSB.

128. The *IoT Labeling NPRM* sought comment on disqualification for nonconformity, referencing the Department of Energy's ENERGY STAR program, which sets out contractual Disqualification Procedures, including a 20 day period to dispute before a formal disqualification decision and what steps an ENERGY STAR partner must take after being formally disqualified (e.g., removing references to ENERGY STAR in the product labeling, marketing).[403] The *IoT Labeling NPRM* asked whether the IoT Labeling Program should adopt a similar process.[404] We agree with EPIC and Planar Systems in supporting a "cure period [to] give[] good actors the opportunity to fix any issues without incurring penalties"[405] and " to address any discovered non-conformance as long as the manufacturer is acting in good faith."[406] Here, we adopt a cure period of 20 days, in line with the ENERGY STAR program.[407]

129. EPIC also supports adopting disqualification procedures similar to ENERGY STAR's for non-compliance, including ceasing shipments of units displaying the label, ceasing the labeling of associated units, removing references to the label from marketing materials, and covering or removing labels on noncompliant units within the brand owner's control.[408] It notes that the EPA also conducts retail store level assessments to identify mislabeled products and argues that a robust enforcement mechanism should include all of these actions.[409] We delegate to the Bureau to consider whether such requirements should follow from termination of authority.

130. In addition, we find that a combination of enforcement procedures for non-compliance are available, including administrative remedies under the Communications Act and civil litigation trademark infringement or breach of contract.[410] Administrative remedies may include, but are not limited to, show cause orders, forfeitures, consent decrees, cease and desist orders, and penalties.[411] The Commission will pursue all available means to prosecute entities who improperly or fraudulently use the FCC IoT Label, which may include, but are not limited to, enforcement actions, legal claims of deceptive practices prosecuted through the FTC, [412] and legal claims for trademark infringement or breach of

[403] *IoT Labeling NPRM* at 20-21, para. 51; *see also* ENERGY STAR, *Disqualification Procedures ENERGY STAR® Products* (Feb. 28, 2018), https://www.energystar.gov/sites/default/files/asset/document/Disqualification_Procedures_0.pdf [https://perma.cc/V4EX-3P8N] (*Disqualification Procedures*).

[404] *IoT Labeling NPRM* at 20-21, para. 51.

[405] *Id.*

[406] Planar Comments at 2.

[407] *See Disqualification Procedures* at 1.

[408] EPIC Reply at 27-31.

[409] *Id.* at 31.

[410] *IoT Labeling NPRM* at 20-21, para. 51.

[411] *Id. See, e.g.*, *Sound Around, Inc.*, Notice of Apparent Liability for Forfeiture, FCC 20-46 (2023) (proposing a $1.2 million penalty for marketing 33 unauthorized RF devices in violation of Section 302 and Section 2.803(b)(1) of the Communications Act of 1934).

[412] In addition, to further help safeguard the integrity of the IoT Labeling Program and the FCC IoT Label, we codify a rule that prohibits any person from, in any advertising matter, brochure, etc., using or making reference to the FCC IoT Label or the Cyber Trust Mark in a deceptive or misleading manner. *See infra*, Appx. A, 47 CFR § 8.212(b). We model our approach on analogous elements of our equipment authorization rules, with which the Commission and industry have substantial experience, and which have proven workable in practice. *See* 47 CFR § 2.927(c).

contract. The record supports both administrative remedies to address consumer harm and civil enforcement actions for false use of the FCC IoT Label.[413] We assert that this combination of enforcement mechanisms are best suited to protect consumer trust in the Cyber Trust Mark and incentivize participant compliance.

131. *Cyber Trust Mark Demonstrates Adherence to Widely Accepted Industry Cybersecurity Standards*. While we decline to preempt state law, we find that approval to use the Cyber Trust Mark on a particular product is an indicator of reasonableness and demonstrates adherence to widely accepted industry standards. The *IoT Labeling NPRM* asked whether the label represented an "indicium of reasonableness" that may serve as a defense or a safe harbor against liability for damages as a result of a cyber incident, while making clear that it did not intend for the IoT Labeling Program to preempt existing laws.[414] While several commenters support Commission preemption of state laws,[415] as well as adoption of liability protections for devices approved to display the Cyber Trust Mark,[416] we decline to preempt state law and decline to implement a legal safe harbor beyond reiterating the Commission's view that achievement of FCC IoT Label is an indicium of reasonableness for entities whose products are compromised despite being approved to use the Cyber Trust Mark. We recognize that a more fulsome safe harbor provision may indeed incentivize participation in the IoT Labeling Program, as the U.S. Chamber of Commerce urges.[417] However, on this record we are not persuaded that it would be feasible or prudent for the Commission to make liability pronouncements as to laws or standards outside the Commission's purview as would be necessary for a broader safe harbor in the absence of preemption. As EPIC observes, such a safe harbor could also decrease consumer trust in the label.[418] In addition, several states have adopted legal safe harbors for entities that implement reasonable security measures (e.g., voluntarily adopt recognized best practices such as NIST's and implement written security programs), and we defer to the states to determine whether approval to use the Cyber Trust Mark meets these State requirements. Given the uncertain interplay between qualification to use the Cyber Trust Mark and various state law regimes, coupled with the risk that such a safe harbor could decrease consumer trust in the label, we decline to preempt state liability requirements at this time.

K. International Reciprocal Recognition of the Cyber Trust Mark

132. The Commission sought comment in the *IoT Labeling NPRM* on how the Commission should coordinate and engage with international bodies maintaining their own labeling programs, and whether to engage in mutual recognition of international labels.[419] We note the robust record highlighting

[413] *See, e.g.*, EPIC Reply at 33 ("Such administrative remedies could include requiring the company to notify impacted consumers, corrective advertising, and financial penalties … [and] we encourage the FCC to take enforcement action or refer the matter to the Federal Trade Commission (FTC) to prosecute under its authority to combat deceptive acts or practices").

[414] *IoT Labeling NPRM* at 21, para. 52.

[415] PMI Comments at 2 (supporting preemption for those states with cybersecurity requirements); CTIA Comments at 36; CTIA Reply at 9 (citing NAM Comments at 6 ("The FCC . . . should limit liability and enhance consistency by providing for preemption of state-level laws and requirements for products participating in the program, and clarifying that the program's legal safe harbor protects companies from potential liability associated with current or future state requirements.")); USTelecom Comments at 11 (urging the Commission to "use its platform as a leading voice in this space to encourage federal preemption," because "[o]pening enforcement to the states will likely cause confusion and inconsistency in application and enforcement").

[416] Chamber Comments at 4; AHAM Comments at 6; Samsung Comments at 5-6; NAM Comments at 6.

[417] Chamber Comments at 2.

[418] EPIC Reply at 35. *See also* Consumer Reports Comments at 28-39 ("[A] safe harbor would mean little in practice, as the company would in any case be required to prove that it had performed all the requisite elements of a robust security program.").

[419] *IoT Labeling NPRM* at 23, para. 55.

the immense value to manufacturers of IoT products in international harmonization of cybersecurity standards.[420] We agree with Widelity that "IoT devices are often manufactured and sold globally. As supply chains evolve, a consistent set of standards will support the rapid growth of innovation and security."[421] We further agree with Consumer Reports that "mutual recognition should only occur when the other program to be recognized has standards as stringent or more stringent" than the IoT Labeling Program.[422]

133. We recognize several other countries already have an established national cyber IoT labeling program, including Singapore,[423] Finland,[424] and Germany.[425] The record cites to these programs and highlights their features for consideration in developing the IoT Labeling Program.[426] For example, the record explains how Singapore's CLS takes reference from the EN 303 645 standards developed by the European Telecommunications Standards Institute (ETSI).[427] We note that other commenters have also recommended use of the ETSI EN 303 645 standards.[428] Further, the record provides Finland's IoT labeling database as an example for developing our IoT registry.[429] Several other countries have government activity around IoT devices or products.[430] For example, Canada has a cybersecurity certification program for small and medium-sized organizations.[431] As another example, South Korea has a IoT security certification system justified under Article 48-6 of their "Act on Promotion of Information and Communications Network Utilization and Information Protection" statute.[432]

134. We also observe continuing developments in IoT security across the globe for consideration. The European Union Agency for Cybersecurity (ENISA) is currently developing a cybersecurity certification framework that would require certain products, services, and processes to

[420] *See* Widelity Comments at 4; Whirlpool Comments at 4-5; AHAM Comments at 4; PTI Comments at 2; American Certification Body, Inc. Reply at 1; Coalition Letter Reply at 2.

[421] Widelity Comments at 4.

[422] Consumer Reports Comments at 40.

[423] Cyber Security Agency of Singapore, *Cybersecurity Labeling Scheme (CLS)*, https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme [https://perma.cc/Z5MR-4TTS] (last visited Dec. 29, 2023).

[424] Finnish Transport and Communications Agency National Cyber Security Centre, *Cybersecurity*, https://tietoturvamerkki.fi/en [https://perma.cc/NF8D-CL97] (last visited Dec. 29, 2023).

[425] Federal Office for Information Security, *IT Security Label*, https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/IT-SiK-fuer-Verbraucher/IT-SiK-fuer-Verbraucher_node.html [https://perma.cc/NS3G-LRFG] (last visited Dec. 29, 2023).

[426] ITI Comments at 6; CSA Comments at 10; TÜV SÜD Comments at 4.

[427] ITI Comments at 6.

[428] Garmin Comments at 10; EPIC Reply at 12.

[429] TÜV SÜD Comments at 4 (providing Finland's IoT labelling database as an example).

[430] *See* Hollie Hennessey & Mike Sullivan-Trainor, Consumer IoT Device Cybersecurity Standards, Policies, and Certification Schemes at Part 1 (2023), https://csa-iot.org/wp-content/uploads/2023/02/Consumer-IoT-Device-Cybersecurity-Standards-Policies-and-Certification-Schemes.pdf [https://perma.cc/UN9M-FE2M].

[431] Government of Canada, *CyberSecure Canada* (Dec. 29, 2023), https://ised-isde.canada.ca/site/cybersecure-canada/en [https://perma.cc/6ZKU-HG9L].

[432] Press Release, Ministry of Science and ICT (MSIT) MSIT and Korea Internet and Security Agency signed an Memorandum of Understanding with the Singapore Cyber Security Agency for Mutual Recognition of IoT Security Certification Systems (Dec. 14, 2023), https://www.msit.go.kr/eng/bbs/view.do;jsessionid=pJsmQ-Zxr72rRsCgyqvwPmVCaAmf3EIfa0FZ60tY.AP_msit_1?sCode=eng&mPid=2&mId=4&bbsSeqNo=42&nttSeqNo=938 [https://perma.cc/CE5P-5EHF].

adhere to specific requirements.[433] Relatedly, the U.S. has signed an agreement for a joint roadmap between the Cyber Trust Mark and similar consumer labeling programs in the EU.[434] Further, Japan has committed to work with the U.S. to "ensure interoperability" of its IoT labeling scheme currently under development.[435]

135. We fully recognize the importance of ensuring international recognition of the IoT Labeling Program and reciprocity considerations underlie our decisions today. We delegate authority to the Bureau and the FCC Office of International Affairs to work with other federal agencies to develop international recognition of the Commission's IoT label and mutual recognition of international labels, where appropriate, as promptly as possible to enable recipients of the Cyber Trust Mark to realize the benefits an internationally recognized Cyber Trust Mark can have to promote global market access. Moreover, the proliferation in the marketplace both in the U.S. and abroad of products meeting a common baseline standard will elevate the overall global cybersecurity baseline for IoT and promote security-by-design approaches to smart products.

L. Consumer Education

136. We adopt the *IoT Labeling NPRM*'s proposal and base the IoT Labeling Program's consumer education requirements on the considerations NIST outlines in the *NIST Cybersecurity White Paper*[436] due to its general applicability to an IoT label and in light of support from the record.[437] The Lead Administrator will be responsible for developing a consumer education campaign that is based on the considerations recommended by NIST in the *NIST Cybersecurity White Paper* and discussed in greater detail below.[438] In developing its consumer education plan, we task the Lead Administrator with considering ways to roll out a robust campaign with a reasonable national reach, including ways to make the consumer education accessible and whether education materials should be developed in multiple languages. We further task the Lead Administrator with considering the costs of conducting such outreach and how that outreach would be funded. Once developed, the Lead Administrator will submit this consumer education plan to the Bureau for consideration and for coordination in publicizing the benefits of the IoT Labeling Program. We recognize the importance of close collaboration between industry and delegate authority to the Bureau to consider and work with the Lead Administrator and other stakeholders to determine how the consumer education campaign would be executed and to execute the campaign. In addition and in furtherance of our expectation that the success of the IoT Labeling Program will be dependent on a close collaboration with the federal government, industry, and other relevant stakeholders,[439] the Commission will coordinate as needed with relevant agencies, such as the Department of Homeland Security, CISA, the FBI, as well as the FTC, the Consumer Product Safety Commission

[433] European Union Agency for Cybersecurity (ENISA), *Cybersecurity Certification Framework*, https://www.enisa.europa.eu/topics/certification/cybersecurity-certification-framework [https://perma.cc/5ZS4-KWTX] (last visited Dec. 29, 2023).

[434] Press Release, European Commission, EU-US Joint Statement on CyberSafe Product Action Plan (Jan. 31, 2024), https://digital-strategy.ec.europa.eu/en/library/eu-us-joint-statement-cybersafe-products-action-plan [https://perma.cc/8D78-H97V].

[435] Press Release, Ministry of Economy, Trade and Industry, Joint Statement of the Japan-U.S. Economic Policy Consultative Committee at 6 (Nov. 14, 2023), https://www.meti.go.jp/press/2023/11/20231116006/20231116006-1.pdf [https://perma.cc/GN7U-PYP4].

[436] *IoT Labeling NPRM* at 22, para. 53; *NIST Cybersecurity White Paper* at 19-20.

[437] *See, e.g.*, CSA Comments at 26; Cybersecurity Coalition Comments at 15; NYC OTI Comments at 4; Comcast Comments at 10; Kaiser Permanente Comments at 5; PMI Comments at 2; NRF Comments at 2; Coalition Letter Reply at 2.

[438] We anticipate that the Lead Administrator may receive support from other Label Administrators in conducting its consumer outreach campaign.

[439] *IoT Labeling NPRM* at 6, para. 9.

(CPSC), and other industry stakeholders who have indicated a willingness to publicize the benefits of the IoT Labeling Program as part of their own consumer education activities.

137. In the *IoT Labeling NPRM*, the Commission stated its expectation that the success of the IoT Labeling Program would require a robust consumer education campaign involving a collaboration with manufacturers, retailers, industry, and non-profit groups to promote the label and explain to consumers what the label means.[440] The Commission sought comment on whether the campaign should rely on consumer education materials recommended by NIST, the anticipated costs of such a campaign, and mechanisms in which to conduct outreach consistent with federal constraints on federal outreach.[441] We agree with CEDIA that consumer education will have a significant impact on meeting the IoT Labeling Program's goals.[442] We further agree that adequate consumer education must inform consumers of the limitations of the Cyber Trust Mark as well as the benefits of having a product that meets baseline cybersecurity requirements,[443] and we agree with CSA that consumers should understand that the label does not guarantee complete device security, but that such protections are an important component of risk management.[444] As pointed out by the City of New York's Office of Technology and Innovation, an effective consumer education program would need to cover the risks and threats to "digital integration of [IoT] devices" and how those risks "can be lessened by helping operators, users, and consumers . . . learn the key elements of a strong IoT Cybersecurity posture."[445] We agree with commenters in the record that NIST's approach to consumer education is best, and note that no commenters opposed NIST's approach.

138. As the Commission acknowledged in the *IoT Labeling NPRM*, NIST has prepared a document identifying consumer education considerations as part of its analysis of a cybersecurity labeling program.[446] In following with NIST's recommendations, the Commission believes consumers should have access to the following information as part of the IoT Labeling Program's consumer education plan:

(1) What the label means and does not mean, including that the label does not imply an endorsement of the product and that labeled products have not completely eliminated risk;

(2) What cybersecurity baselines must be met to obtain authority to affix the label, why they were included, and how those criteria address security risks;

(3) A glossary of applicable terms, written in plain English;

(4) General information about the conformity assessment process, including information about how the conformity assessment was conducted and the date the label was awarded to the product;

(5) The kinds of products eligible for the label and an easy way for consumers to identify labeled products;

(6) The current state of device labeling as new cybersecurity threats and vulnerabilities emerge;

[440] *Id.*at 21, para. 53.

[441] *Id.*at 21-22, paras. 53-54.

[442] CEDIA Reply at 5 ("Consumer and industry education will have a significant impact on meeting the goals of the U.S. Cyber Trust Mark program.").

[443] *See id.*("[E]ducation must also inform consumers of the limitations of the mark; and that 'reasonable efforts' alone may not fully protect the consumer.").

[444] CSA Comments at 18 ("No IoT device will be completely secure . . . . Nevertheless, cybersecurity features, like seatbelts and airbags in cars, are beneficial in reducing risk.").

[445] NYC OTI Comments at 4.

[446] *IoT Labeling NPRM* at 21-22, para. 53; *NIST Cybersecurity White Paper* at 19-20.

(7) Security considerations for end-of-life IoT products and functionality implications if the product is no longer connected to the Internet;

(8) Consumer's shared responsibility for securing the device software and how their actions (or inactions) can impact the product's software cybersecurity; and

(9) Contact information for the IoT Labeling Program and information on how consumers can lodge a complaint regarding a product label.

139. We recognize that some aspects of this consumer education campaign overlap other aspects of the IoT Labeling Program, such as the registry. We see no harm with including that information in the registry as well as the consumer education campaign. We also observe the importance of conducting what NIST describes as a "campaign" to establish and increase label recognition,[447] and thus envision a Lead Administrator-led, multiple stakeholder engagement that puts NIST's recommendations into practice.

140. NIST has conducted research into the consumer perspective on the loss of manufacturer support in IoT products.[448] The research suggests that proactive communication to consumers from the manufacturer with information about end-of-life support policies, the expected lifespan, and how to sign up for notifications about changes to support is an additional, important step.[449] NIST also emphasizes the importance of consumer education about the meaning of the dates attached to a label, and cautions that this can confuse consumers as to the date's meaning.[450] We agree with Consumer Reports that educating consumers about the meaning of support periods is an important aspect of consumer education.[451] We believe that the recommendations identified by NIST in the *NIST Cybersecurity White Paper*, coupled with the consumer research done by NIST and industry, provide a strong model that the Lead Administrator can utilize in its consumer education campaign to meet the goals NIST and the record, discussed above, identify as important for a successful consumer education campaign.

141. To assist the Lead Administrator in promoting consumer education, the Commission will coordinate publicizing the benefits of the IoT Labeling Program with the relevant agencies, including the Department of Homeland Security, CISA, FBI, FTC, the Consumer Product Safety Commission (CPSC), and other industry stakeholders who have indicated a willingness to assist with consumer education. A coalition of trade associations advocates for a consumer education program led by the U.S. government,[452] but do not propose how to conduct outreach consistent with the federal outreach concerns articulated in the *IoT Labeling NPRM*.[453] We agree that a government outreach program is essential in a larger campaign to effectively inform consumers about the IoT Labeling Program, consistent with NIST's recommendations identified above. The Commission intends to work closely with CISA to make use of their "Secure our World" program.[454] We agree with CTA that federal consumer education efforts do not preclude independent communication and outreach programs.[455] For example, the National Retail

[447] *NIST Cybersecurity White Paper* at 19.

[448] *See NIST Consumer Perspectives Research*.

[449] *Id.*at 502-503.

[450] *Id.*at 503.

[451] Consumer Reports Comments at 26 ("Relatedly, we will have to educate consumers that a connected device required regular updates over time in order to stay secure.").

[452] Coalition Letter Reply at 4.

[453] *IoT Labeling NPRM* at 21, para. 53.

[454] Cybersecurity & Infrastructure Security Agency, *Secure Our World*, https://www.cisa.gov/secure-our-world [https://perma.cc/4KFU-RSGC] (last visited Jan. 12, 2024).

[455] CTA Comments at 32 ("The private sector can augment the government's educational campaign through advertising, websites and social media.").

Foundation indicated their willingness to support consumer education efforts.[456] While Everything Set, Inc. is concerned that outsized private sector involvement in consumer education might hurt the campaign's credibility,[457] we believe that retail and manufacturer involvement in promoting the IoT Labeling Program and the limitations of the IoT Labeling Program are important to ensure widespread recognition of the Cyber Trust Mark in commerce. To promote consumer education and engage in a joint effort with industry and stakeholders to raise awareness of the label, the Commission will coordinate with the Lead Administrator, Executive Agencies, and other industry stakeholders who have indicated a willingness to publicize the benefits of the IoT Labeling Program as part of their own consumer education efforts.

M. Cost/Benefit Analysis

142. Our analysis indicates that the expected benefits of the IoT Labeling Program greatly exceed the expected costs of the program. The expected benefits of the IoT Labeling Program include improved consumer cyber awareness; reduced vulnerability of products that could be used in cyberattacks both in people's homes and as part of a larger national IoT ecosystem; and increased manufacturer competition and relational benefits stemming from increased goodwill and product awareness. Consumers value the security of their devices, and the complexity of understanding whether IoT devices meet baseline security standards, and making informed purchases on that basis is a significant cost to consumers.[458]

143. *Consumer Benefit from Reduced Search Costs*. The Cyber Trust Mark can lower consumer research costs by reducing the amount of time consumers spend researching the cybersecurity characteristics of IoT products before making a purchase. We estimate that the Cyber Trust Mark will save consumers at least $60 million annually from reduced time spent researching cybersecurity features of potential purchases. We use the U.S. Department of Transportation (DOT)'s approach of valuing the time savings of travel to value the time savings to consumers of the Cyber Trust Mark.[459] Our analysis relies on the share of households with a smart home device (which we note is only one segment of the IoT market likely to be impacted by this Order), the share of those households that are likely to devote time to investigating the cybersecurity of their connected products, and an estimate of their time value of researching cybersecurity characteristics of devices. First, we estimate that 49 million U.S. households own at least one IoT device from a market segment that likely will be impacted by the Cyber Trust Mark. Further, recent survey evidence suggests that 32% of households are invested in reducing their

[456] *See* NRF Comments at 2 ("The National Retail Foundation . . . supports the idea that retailers who sell IoT devices should be part of broader efforts to raise consumer awareness around IoT cybersecurity.").

[457] Everything Set, Inc. Comments at 3.

[458] Summary statistics from American Experiences Survey conducted by Consumer Reports found that the majority of respondents were interested in purchasing a connected device and a large share had difficulty learning about the security features of connected devices. *Consumer Reports Summer Research* at 5 ("Four out of five of our respondents were interested in purchasing a connected device scoring their desire between 3 and 5 on a five-point scale with 5 being most interested, and 38% had tried to find security or privacy information about a connected device before purchase. But many found it difficult because it was either unavailable, available only after purchase, buried on legal documents, or not always found in a consistent place."). Similarly, Comcast highlights the difficulty consumers have comparing security features between products. Comcast Comments at 10 ("But today there is an information asymmetry: consumers do not have a reliable, easy-to-understand mechanism to compare security features between otherwise comparable IoT devices (or, as noted, to understand that a device's security is no longer being supported.)").

[459] *See* Memorandum from Vinn White, Acting Assistant Secretary for Transportation Policy, U.S. Department of Transportation to Secretarial Officers and Modal Administrators at 13 (Sept. 27, 2016), https://www.transportation.gov/sites/dot.gov/files/docs/2016%20Revised%20Value%20of%20Travel%20Time%20Guidance.pdf [https://perma.cc/MP3R-TMS7].

cybersecurity risk.[460] We estimate each hour of time savings to be valued at $16 based on the median compensation in the U.S. and an individual's potential preference for researching products rather than working an additional hour.[461] We note that this calculation only focuses on one segment of the IoT market, which may underestimate the time savings induced by this Order. We recognize that the exact time savings of utilizing the Cyber Trust Mark relative to searching for information online is unknown, so a lower end estimate of 15 minutes of time savings per year per household is used. We find a 15-minute time savings is consistent with the value of cybersecurity features disclosed in surveys.[462] Given manufacturer and industry group comments showing support for consumer awareness and cybersecurity, we believe there would be sufficiently large enough immediate manufacturer participation in the IoT

[460] A survey of households showed that 41% of internet connected households (92%) have a smart home device. This indicates that 38% (=92%*41%) of households have at least one smart home device. The survey represented the market for smart home devices, like thermostats, lighting control systems, smart appliances, and other components. *See* Jennifer Kent, Next-Generation Smart Home: Building for the Future at 2, https://www.parksassociates.com/products/whitepapers/next-gen-smart-home-2023 [https://perma.cc/KJE6-T3EW] (last visited Jan. 18, 2024). This would indicate that out of the 130 million households in the United States, 49 million (=130,000,000*0.38) have an IoT device. *See* U.S. Census Bureau, *Selected Social Characteristics in the United States (DP02) American Community Survey 2022 1-Year Estimates*, https://data.census.gov/table?q=households&g=010XX00US [https://perma.cc/3YZ5-XFM8] (last visited Feb. 8, 2024). Furthermore, a survey by Cisco shows that 32% of consumers are "Privacy Actives" - those that are interested in privacy and security and have acted on behalf of those interests. *See* Cisco, Building Consumer Confidence Through Transparency and Control at 5 (2021), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf?CCID=cc000742&DTID=esootr000515&OID=rptsc027438 [https://perma.cc/2KHM-K978]. This indicates that 15 million (=130,000,000*0.38*0.32) (rounded down) households would experience cost savings from using the Cyber Trust Label.

[461] The median wage is $22.46 for all occupations and it is adjusted by 1.45 = ($43.93/ $30.35), which is the ratio of average total compensation to average wages to fully account for the benefits of an additional hour of work. U.S. Bureau of Labor Statistics, *May 2022 National Occupational Employment and Wage Estimates* (Apr. 25, 2023), https://www.bls.gov/oes/current/oes_nat.htm#00-0000; Press Release, U.S. Bureau of Labor Statistics, Employer Costs for Employee Compensation – September 2023 (Dec. 15, 2023), https://www.bls.gov/news.release/pdf/ecec.pdf. Value of time savings calculations are dependent on an individual's willingness to pay a portion of their hourly income to avoid an activity. Generally, the more uncomfortable the activity the larger the share of income an individual would pay. DOT uses 50% for personal local travel, meaning an individual would be willing to pay half of their hourly income to avoid one hour of personal travel, and 70% for personal intercity travel. The rate at which consumers are willing to pay to avoid spending an hour of time researching cybersecurity concerns is unknown so the preference associated with personal local travel (50%) is used. *See* Memorandum from Vinn White, Acting Assistant Secretary for Transportation Policy, U.S. Department of Transportation to Secretarial Officers and Modal Administrators at 13 (Sept. 27, 2016), https://www.transportation.gov/sites/dot.gov/files/docs/2016%20Revised%20Value%20of%20Travel%20Time%20Guidance.pdf [https://perma.cc/MP3R-TMS7]. Given the difficulty in researching IoT security that is highlighted by the record, we believe this preference rate is reasonable. Together this means that each hour of time savings is equal to $16.14 (=22.26*1.45*0.5).

[462] We find the value of 15 minutes of search time to be consistent with the value consumers already place on various security features. For example, a survey related to smart home devices found that participants were willing to pay $5.75 for automatic updates relative to manual security updates. From the same survey consumers were also willing to pay $12.74 for password protection. Given that an hour of research time is valued at $16.14, it is likely that a household would be willing to spend at least 15 minutes, valued at $4.04= (16.14/(15/60)) researching whether a device has the security features they are interested in. *See* Pardis Emami-Naeini et al., *Are Consumers Willing to Pay for Security and Privacy of IoT Devices?*, USENIX (Aug. 2023), https://www.usenix.org/conference/usenixsecurity23/presentation/emami-naeini [https://perma.cc/SYJ7-W4QA] (*Duke and Carnegie Mellon Study*).

Labeling Program to incur these benefits in the first year of the program, and every year thereafter.[463] Nationwide, the Cyber Trust Mark would result in a minimum of $60 million in time savings annually.[464]

144. A separate approach to calculating the benefit of the Cyber Trust Mark is to estimate the value consumers place on security and privacy features of IoT devices. A study submitted by Consumer Reports found that respondents valued individual security upgrades between $6 and $13.[465] The study also found that devices were valued at around $34 more if they had a label emphasizing a bundle of the most protective security features.[466] Given the difficulty consumers face in understanding what security and privacy features are included in a device, the Cyber Trust Mark would help consumers easily identify and choose products with features they value. For example, if the Cyber Trust Mark represented the most protective features associated with the label in the in the study, a consumer would benefit by $34 from purchasing a device with the Cyber Trust Mark over a device that did not display the Mark. Based on our estimate of 15 million households that would be impacted by the IoT labeling program, we estimate that the benefit to consumers, in terms of the added value of the Cyber Trust Mark, would be between $85 million and $500 million annually.[467] While the exact security features that will be proposed by the Lead Administrator in collaboration with stakeholders are not yet determined, if the Cyber Trust Mark only emphasized the lowest valued security feature, the program would produce a benefit of at least $85 million.[468]

145. *Manufacturer Competitive and Reputational Benefits*. Aside from the direct benefits to consumers, there are also wider benefits of the Cyber Trust Mark. Participating businesses benefit from product differentiation and quality signaling vis-a-vis competitors that do not participate in the IoT

[463] Cisco Comments at 1 ("Cisco shares the Commission's goal of increasing consumer awareness of cybersecurity concerns related to IoT and we have a significant interest in strengthening the resiliency of the communications network."); Samsung Comments at 2 ("Samsung is also committed to strengthening IoT security through leadership in industry initiatives and standard-setting bodies."); AHAM Comments at 1 ("AHAM conceptually supports the Commission's effort to create a voluntary program that allows manufacturers to show that they took the necessary steps to meet a baseline standard of security for IoT products"); CTA Comments at 2 ("CTA and its members have made enhancing security across the IoT ecosystem a top priority. In 2018, CTA joined forces with partners across the connected ecosystem to form the Council to Secure the Digital Economy (CSDE) and develop guidance for the international information and communications technology community on how to secure IoT and reduce risk across the connected ecosystem.").

[464] $60 million = (15,000,000*$16*(15/60)) is the estimated value for 15 minutes of time savings nationwide.

[465] *See Duke and Carnegie Mellon Study* at 8, Table 2. Researchers calculated consumers' willingness to pay for five individual security and privacy improvements related to a smart speaker with voice assistant and a smart smoke detector. The security features varied from low protection to high protection. On the high end, Table 2 shows that consumers were willing to pay $13.31 for cloud storage to be de-identifiable verse identifiable. On the low end, consumers were willing to pay $5.75 for automatic security updates verses manual ones.

[466] Researchers calculated consumers' willingness to pay for a device with no label verses a device with a label indicating the device included a set of the most protective security features. *See id.* ("The regression analysis (see Table 4) showed that compared to having risky security and privacy practices or no transparency, participants were significantly more willing to purchase . . . and willing to pay significantly higher premiums (. . . premium= $33.63 . . .) to have a smart device with improved security and privacy practices.").

[467] As noted in our analysis above, there are approximately 15 million households that would benefit from being aware of their IoT devices cybersecurity. The range of benefits is based on the range of values discussed in the *Duke and Carnegie Mellon Study*. Based on the lowest valued feature the benefit would be $85 million ≈ (15,000,000*$5.75) and based on the value of the label, the higher end of benefits would be $500 million ≈ (15,000,000*$33.63), with both estimates rounded down to the nearest five million.

[468] Consumers valued automatic updates over manual updates at a value of $5.75. This is the lowest value feature that consumers still put a positive premium on. *See Duke and Carnegie Mellon Study* at 8, Table 2. While we understand that some devices that consumers are already purchasing contain the features they value, by focusing on the lower end of benefits, we emphasize the lower bound of value placed on security and privacy features.

Labeling Program and from increased company goodwill and reduced risks related to cybersecurity incidents.[469] By aligning minimum security practices with the proposed standards, and communicating those standards to consumers, manufacturers may be able to generate goodwill and reduce business loss after cybersecurity incidences.[470] While we do not revisit our discussion of a safe harbor from liability as discussed above, we note that manufacturers may benefit from adopting security practices that are consistent with standards necessary to bear the Cyber Trust Mark. We highlight that there have been several instances where the Federal Trade Commission investigated and settled with firms due to poor security practices or inaccurate communication of their security practices.[471] We merely note that a manufacturer that has gone through the process of obtaining the Cyber Trust Mark may benefit from likely having documented the security practices and attendant testing necessary to acquire the Mark.

146. *Market-Wide Benefits of Reduced Cybersecurity Incidents.* Insecure IoT products are often used in distributed denial-of-service (DDoS) attacks, which can be used to overwhelm websites to create a distraction during other cybersecurity crimes, or to request a ransom be paid to stop the attack. While we cannot quantify the expected benefits the Cyber Trust Mark may have on reducing the number of vulnerable devices and/or the potential reduction on their likelihood of being used in a cybersecurity attack, commenters do highlight improved security as one of the major benefits of this IoT Labeling Program.[472] We do further emphasize this as a benefit that is likely to have significant impacts on firms in a wide range of industries.[473]

147. *Costs to IoT Labeling Program Participants*. Only those entities who choose to participate will incur costs associated with the voluntary IoT Labeling Program. The specific costs of to participating manufacturers cannot be readily measured but are expected to include: conformity testing

[469] Consumers value cybersecurity and the Cyber Trust Mark would help them identify devices/products that are consistent with their preferences. Research found that consumers were willing to pay a premium for cybersecurity features and many searched for device cybersecurity information before purchase. *See id.*at 1 ("Participants were willing to pay a significant premium for devices with better security and privacy practices."); *Consumer Reports Summer Research* at 5 ("Four out of five of our respondents were interested in purchasing a connected . . . and 38% had tried to find security or privacy information about a connected device before purchase.").

[470] A report by IBM includes reputational costs as a factor associated with lost business that can be associated with a data breach. IBM Security, Cost of a Data Breach Report at 15 (2023), https://www.ibm.com/downloads/cas/E3G5JMBP [https://perma.cc/5NMF-5HQE] ("Lost business costs include activities such as business disruptions and revenue losses from system downtime, the cost of lost customers and acquiring new customers, and reputation losses and diminished goodwill."); *see also* Duke and Carnegie Mellon Study at 1 ("Participants were willing to pay a significant premium for devices with better security and privacy practices.").

[471] "The FTC also alleged that Tapplock failed to implement a security program or take other steps that might have helped the company discover electronic vulnerabilities with its locks." Press Release, FTC, FTC Gives Final Approval to Settlement with Smart Lock Maker (May 20, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/05/ftc-gives-final-approval-settlement-smart-lock-maker [https://perma.cc/RQ3P-GWV5]. "According to the complaint, Ring also failed to implement standard security measures to protect consumers' information from two well-known online threats—"credential stuffing" and "brute force" attacks—despite warnings from employees, outside security researchers and media reports." Press Release, FTC, FTC Says Ring Employees Illegally Surveilled Customers, Failed to Stop Hackers from Taking Control of Users' Cameras (May 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users [https://perma.cc/P5MN-RCJC].

[472] *See, e.g.*, Keysight Comments at 1; Logitech Comments at 1; A2LA Comments at 1; AIM Comments at 1; Widelity Comments at 1; Whirlpool Comments at 3; ITI Comments at 2; Everything Set, Inc. Comments at 3.

[473] Industry reports highlight the use of IoT devices in DDoS attacks as well as the potential harm of such attacks. *See* Akamai, *The Evolution of DDoS: Return of the Hacktivists* at 4 (Jan. 2023), https://www.akamai.com/resources/research-paper/the-evolution-of-ddos-return-of-the-hacktivists [https://perma.cc/VT6H-4KZ8] ("The explosion of the Internet of Things (IoT) has been a boon to DDoS attackers, providing an endless army of poorly secured devices that they can requisition to serve as botnets.").

fees at a CyberLAB, CLA lab, or through in-house testing; CLA fees; internal compliance and filing costs; Cyber Trust Mark placement on product; costs incurred for API access as part of the QR Code; a customer information campaign; and adjustments to security practices necessary to meet the standards established for the Cyber Trust Mark. These costs are likely to vary depending on the standards and testing procedures proposed by the Lead Administrator as well as the extent of manufacturer participation. Any in-house testing lab will also be required to obtain accreditation to ISO/IEC standards and will incur the accreditation costs. We expect that manufacturers that choose to pursue this option may offset the accreditation costs with time savings, and potentially cost savings, associated with in-house testing.

148. Participating manufacturers will incur conformity testing, reporting costs, potential renewal fees, and Label Administrator processing fees, but the Commission's IoT Labeling Program is voluntary and we only expect manufacturers who would benefit from the program to participate in the long-run, further indicating that accrued benefits will exceed manufacturer costs. Furthermore, comments in the record show that many manufacturers and industry groups are in favor of consumer awareness and addressing cybersecurity concerns.[474] This provides some indication that manufacturers perceive the benefits of participating in the IoT Labeling Program as outweighing the costs. We understand that manufacturers' security practices for IoT products vary. Some manufacturers will find it beneficial to align their cybersecurity standards with the IoT Labeling Program's standards and apply for the Cyber Trust Mark. If a manufacturer decides not to participate in the program, then they will not experience any additional costs.

149. *Cost of Registry Development and Administration*. We attempt to estimate the cost of developing and administering the registry with currently available information, recognizing that our cost estimate is unable to incorporate pending issues that will be addressed by the Bureau as discussed above.[475] While the cost to the Lead Administrator to manage the registry in accordance with the Bureau's pending determinations and as discussed above are forthcoming, we nevertheless attempt to estimate the costs of the Lead Administrator' administrative role in managing the registry as described above. Our estimate utilizes data submitted by Consumer Reports, which envisioned a centralized registry. We note that the registry, as adopted, will be less burdensome than the costs described by Consumer Reports in their estimates.[476] Our estimate to maintain registry components and review applications as part of the CLA duties, which aligns with the middle of the expert range based on commenter submissions, is approximately $5 million annually. The high-end estimate submitted by Consumer Reports is $10 million.[477] Consumer Reports indicates that setting up a centralized registry could be done by one individual with a few contractors at a cost less than $200,000 a year.[478] Depending on the requirements, the Lead CLA may still need to set up some minimal components of a registry and incur a small portion of these costs. The estimates on the annual administration costs are much less precise with the expert proposed estimate of between $100k and $10 million annually, with indication that the $10 million estimate is on the very high end.[479] Staff calculate a more reasonable, but likely still high, estimate in the middle of that range, even accounting for the advanced technical expertise that would be required to review applications. For example, an organization relying on five lawyers, five electrical

[474] *See, e.g.*, Cisco Comments at 1; Samsung Comments at 2; AHAM Comments at 1; CTA Comments at 2; Coalition Letter Reply at 1.

[475] *See supra* para.121.

[476] The Consumer Reports proposed registry architecture includes a dataset that can store images and PDFs as well as allows for device manufacturers, retailers, security researchers and administrators to access the platform. *See Consumer Reports Registry Design Proposal* at 4. The registry, as adopted, does not include these features and therefore would not incur the costs to develop and maintain them.

[477] *Id.* at 7.

[478] *Id.*

[479] *Id.*at 8.

engineers, and five software developers in a full-time capacity would require $3 million annually in wage compensation. If we generously assume another $2 million in additional costs to accommodate ISO/IEC accreditation, contractors, facilities, and other resources, the total is $5 million. While these estimates are for a single administrator, we believe this is a reasonable estimate of the staffing costs that would be distributed among the CLAs to meet the requirements of reviewing applications.

150. The estimated high-end costs of administering the IoT Labeling Program annually ($10 million) are far less than the low-end estimate of annual benefits to consumers ($60 million) of just one aspect of the program. We further highlight that the benefits to manufacturers are likely to exceed manufacturer's participation costs. Together this indicates the total program benefits exceed costs. Because the initial startup costs are so low relative to the benefits, we do not compare the discounted values.

IV. LEGAL AUTHORITY

151. We adopt the *IoT Labeling NPRM*'s tentative conclusion that the FCC has authority to adopt the IoT Labeling Program. We conclude that section 302 provides us with the authority to adopt a voluntary program for manufacturers seeking authority to affix the FCC-owned Cyber Trust Mark on wireless consumer IoT products that comply with the program requirements.[480] In the *IoT Labeling NPRM*, the Commission sought comment on its authority under section 302 of the Act, along with other possible sources of authority.[481] In particular, under section 302(a) of the Act, consistent with the public interest, convenience, and necessity, the Commission is authorized to make "reasonable regulations (1) 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; and (2) establishing minimum performance standards for home electronic equipment and systems to reduce their susceptibility to interference from radio frequency energy.'"[482]

152. Some commenters question our authority under section 302 to establish an IoT Labeling Program.[483] The U.S. Chamber of Commerce cautions the Commission to not "overinterpret its harmful interference authority" under sections 302(a) and 333.[484] CTIA argues that the Commission does not have the authority to regulate cybersecurity, but does not cite to section 302(a) or explain why the Commission's action today does not fall within the scope of section 302(a) or any other section of the Communications Act.[485] Others do not dispute the Commission's authority to adopt a voluntary program but argue that the Commission does not have the authority to make the IoT Labeling Program mandatory.[486]

[480] 47 U.S.C. § 302a.

[481] *IoT Labeling NPRM* at 23-26, paras. 57-65.

[482] 47 U.S.C. § 302a(a).

[483] *See, e.g.*, NTCA Comments at 10 ("It is not clear that a voluntary IoT label program intended to increase consumer confidence serves the explicit concerns of diminishing radio interference as contemplates in Sections 302(a) and 333."); CTIA Comments at 43 ("[T]he FCC does not have any express statutory authority to create a cybersecurity labeling program or otherwise adopt requirements related to the cybersecurity of Internet-connected devices."); Chamber Comments at 3 ("The Chamber is concerned with the Commission's interpretation of its legal authority.").

[484] Chamber Comments at 3.

[485] CTIA Comments at 42-44.

[486] *See* USTelecom Comments at 2 ("[S]ections 302 or 333 of the Communications Act do not authorize the Commission to impose general cybersecurity *requirements* . . . .") (emphasis added); *see also, e.g.*, NCTA Comments at 13 n.27 ("Although NCTA previously raised concerns about the scope of the Commission's authority under Section 302 to address cybersecurity concerns in other contexts, here the Commission proposes to establish a

(continued….)

153. We agree with Comcast that Congress intended section 302 to be flexible enough "to address novel issues not yet on the legislative radar[.]"[487] As Comcast further observes, "[t]he stated goal of the [IoT Labeling] Program is to 'ensure that IoT devices have implemented certain minimum cybersecurity protocols to prevent their being hacked by bad actors who could cause the devices to cause harmful interference to radio communications," which falls squarely within the Commission's remit under Section 302(a)."[488] Further, NYC OTI points out that IoT which "by design doesn't protect against the reception of spurious or unintended RF communications may be subject to a series of radio-layer attacks due to the lack of these protections" and thus is within our authority to regulate.[489] A voluntary IoT Labeling Program thus assures consumers that certain cybersecurity standards are met to protect those devices from being used to generate interference to other devices.[490]

154. In addition to our authority under section 302(a)(1), section 302(a)(2) authorizes the Commission to "establish minimum performance standards for home electronic equipment and systems to reduce their susceptibility to interference from radio frequency energy."[491] A voluntary program for consumer IoT products is encompassed within our authority to regulate home electronic equipment and their accompanying systems that render that home electronic equipment operational.

155. Section 302(a)(2) allows such regulations to apply to "the manufacture, import, sale, offer for sale, or shipment of such devices and home electronic equipment and systems[.]" The legislative history of section 302 also supports our conclusion. Congress adopted section 302 due to concerns about radio frequency interference to consumer electronic equipment:[492]

> In the market for home devices, however, good faith industry attempts to solve this interference have not always been as successful. . . . [T]he Conferees believe that Commission authority to impose appropriate regulations on home electronic equipment and systems is now necessary to insure that consumers' home electronic equipment and systems will not be subject to malfunction due to [radio frequency interference].[493]

156. Congress envisioned "home electronic equipment and systems" to include not only radio and television sets, but all types of electronics and their supporting systems used by consumers.[494] Examples given by Congress were home burglar alarms, security systems, automatic garage door openers,

voluntary program that is limited to connected devices, which is well within the Commission's Section 302 and 333 authority."); CTIA Reply at 4-5 (noting that "several commenters articulated their view that while a voluntary program could be considered 'reasonable,' the FCC lacks authority to develop mandatory regulations or requirements under Sections 302, 303, or 333 of the Act," and observing that "a purely voluntary program is unlikely to invite the same scrutiny as a set of mandatory standards"). Because we adopt a voluntary program, we need not address arguments that it would be unreasonable under section 302(a) to adopt mandatory requirements or that mandatory requirements otherwise would be beyond the Commission's authority.

[487] Comcast Comments at 15.

[488] *Id.* at 14 (quoting *IoT Labeling NPRM* at 24, para. 59); *see also, e.g.*, NCTA Comments at 12-13.

[489] NYC OTI Comments at 4-5.

[490] *See* Zhifei Xu *et al.*, *Inaudible Attack on Smart Speakers With Intentional Electromagnetic Interference*, Vol. 69 IEEE Transactions on Microwave Theory and Techniques (2021). While CTIA asserts that "[a]ttacks that seek to weaponize radiofrequency interference . . . are not a major risk" it does not provide the basis for that assertion—and even it concedes that such attacks are possible. CTIA Reply at 4. Based on our historical experience and expertise we are more cautious about such risks and believe the voluntary IoT Labeling Program we adopt for Internet-connected wireless devices is a measured response appropriately calibrated to our assessment of those risks.

[491] 47 U.S.C. § 302a(2).

[492] H.R. Rep. No. 97-765, at 32 (Conf. Rep.), 1982 U.S.C.C.A.N. at 2276 (1982).

[493] Conf. Rep. at 2276.

[494] *Id.*

record turntables, and sound systems.[495] Congress clearly foresaw interference and disruption to consumer equipment and the systems that equipment was connected to as within the ambit of section 302 when it gave the Commission "exclusive jurisdiction" over matters involving radio frequency interference.[496] The many alternatives available to the Commission to accomplish its duty under section 302 include directing manufacturers to meet "certain minimal standards" or utilizing labels.[497]

157. We additionally conclude that our section 302(a) authority to adopt "reasonable regulations" governing the interference potential of devices capable of causing RF interference empowers us to choose specific approaches that advance goals of the Act in addition to the core concerns in section 302(a)(1) and (2).[498] For one, as widely supported in the record, we rely on NIST's recommended IoT criteria (the NIST Core Baseline) as the foundation for the cybersecurity requirements to be applied under the IoT Labeling Program.[499] Even if some elements or applications of those criteria could advance policies or interests in addition to guarding against the risk that exploited vulnerabilities in Internet-connected wireless consumer IoT products could cause harmful interference, it would be neither prudent nor workable to try to segregate or disaggregate that package of criteria in an effort to isolate some product capabilities from others in an effort to narrow the Program's focus. To the contrary, maintaining the integrity of the cohesive package of NIST criteria advances the directive in section 302(a) to address the interference potential of wireless devices through "reasonable regulations."[500] Commenters point out, for example, that even when harmful interference to IoT products from cyberattacks "is not necessarily the traditional form of interference caused by devices operating in frequencies and at power levels not approved by the Commission[,]" it can implicate statutory policy concerns nonetheless.[501] Under the circumstances here, we thus find it "reasonable" for our IoT Labeling Program to rely on the full package

[495] *Id.*

[496] *Id.*

[497] *Id*. at 2277.

[498] We thus reject claims to the contrary. *See, e.g.*, NTCA Comments at 7-8.

[499] We reject the efforts of some commenters to cast doubt on our authority by arguing that "[t]o date, the Commission has not played a role in reviewing IoT for cybersecurity risks, and Congress did not look to the Commission when it considered and passed legislation to improve IoT cybersecurity." Chamber Comments at 3. But there is no doubt that Congress has looked to NIST in that regard. *See, e.g.*, *IoT Cybersecurity Improvement Act of 2020*, 15 U.S.C. § 278g-3a to § 278g-3e (establishes minimum cybersecurity requirements for IoT technology procured by the U.S. government and directs federal agencies to only procure devices that comply with NIST guidelines (NIST SP 800-213 and 213A) and establishes vulnerability reporting requirements for products sold to the U.S government); *see also* CTIA Comments at 11-12 (citing the *IoT Cybersecurity Improvement Act of 2020* and noting that it "delegated authority to NIST and the Department of Homeland Security"). It remains proper for us to carry out our statutory duties even when they implicate issues that some might argue historically have not been as central a focus of the Commission's work, and it is eminently reasonable for us to do so informed by outside expertise—as reflected in our reliance on the NIST Core Baseline as the foundation for our IoT Labeling Program, and through our public-private collaboration efforts here more generally. *Cf. Huawei Tech. USA, Inc. v. FCC*, 2 F.4th 421, 427 (5th Cir. 2021) ("Assessing security risks to telecom networks falls in the FCC's wheelhouse. And the agency's judgments about national security receive robust input from other expert agencies and officials. We are therefore persuaded that, in crafting the rule, the agency reasonably acted within the broad authority Congress gave it to regulate communications."); *id*. at 439 ("[T]he FCC cannot conjure national security authority out of thin air. . . . [B]ut as the FCC argues, the Act's purposes include 'mak[ing] [communication] available . . . for the purpose of the national defense' and 'promoting safety of life and property through the use of wire and radio communications.' The agency reasonably read 'public interest' in light of these larger goals to encompass secure networks." (citation omitted)).

[500] 47 U.S.C. § 302a(a).

[501] Comcast Comments at 15; *see also, e.g.*, NYC OTI Comments at 4-5 (IoT which "by design doesn't protect against the reception of spurious or unintended RF communications may be subject to a series of radio-layer attacks due to the lack of these protections.").

of IoT cybersecurity criteria that guard against the risk that the covered products *cause* harmful interference, and also guard against the risk of interference *to* those covered products—even in the case of non-RF interference—consistent with the policy goals underlying provisions such as sections 302(a) and 333 and of the Act.[502] Our understanding of the reasonableness of our approach here also is informed by the public safety and national security goals in sections 1 and 4(n) of the Act.[503] Thus, although we do not rely on additional provisions beyond section 302 as authority for the voluntary IoT Labeling Program we adopt today, they inform our understanding of what regulatory approach to implementing section 302(a) is reasonable under these circumstances.[504]

158. Comcast also cites the legislative history of section 302(a) in support of our authority to establish an IoT Labeling Program.[505] Congress agreed with a letter from the Commission that initial language that would have restricted section 302(a) to devices that cause harmful interference to "'commercial, aircraft, and public safety' radio communications" was too narrow.[506] Congress instead adopted the current language: "reasonable regulations . . . consistent with the public interest, convenience, and necessity."[507] The Commission's authority under section 302 was designed by Congress to be "sufficiently broad to permit it to formulate rules relating to any service where interference from these devices is a serious problem."[508] Such language, it was believed, would be "sufficiently broad to permit it to formulate rules relating to any service where interference from these devices is a serious problem."[509] We conclude that a voluntary program with minimum standards to prevent radio interference to consumer IoT products is consistent with the text and history of section 302.

159. Further, we have previously imposed security requirements that prevent unauthorized parties from accessing and alerting technology to cause radio interference under our section 302 authority. In 2020, we required that access points to automated frequency coordination systems were secure so unauthorized parties could not alter the list of available frequencies and power levels sent to an access point.[510] We agree with Comcast that our previous actions requiring end user devices to "contain security features sufficient to protect against modification of software and firmware by any unauthorized parties"[511] and actions to secure unlicensed national information infrastructure devices[512] are sufficiently analogous to this proceeding as to be supported by our section 302 authority.[513]

[502] 47 U.S.C. §§ 302a(a), 333.

[503] 47 U.S.C. §§ 151, 154(n).

[504] Because we conclude that section 302 of the Act authorizes our actions today, we defer consideration of other sources of authority that the Communications Act may grant the Commission over this area.

[505] Comcast Comments at 14.

[506] U.S. Rep. No. 90-1276, at 7 (1968), *reprinted in part at* 114 Cong. Rec. 18,428 (June 24, 1968).

[507] *Id.*; 47 U.S.C. § 302a.

[508] U.S. Rep. No. 90-1276, at 7 (1968), *reprinted in part at* 114 Cong. Rec. 18,428 (June 24, 1968).

[509] *Id.*

[510] *Unlicensed Use of the 6 GHz Band; Expanding Flexible Use in Mid-Band Spectrum Between 3.7 GHz and 24 GHz*, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3852, para. 79 (2020).

[511] *Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550- 3650 MHz Band*, GN Docket No. 12-354, Report and Order and Second Further Notice of Proposed Rulemaking, 30 FCC Rcd 3959, 4033-4034, para. 240 (2015).

[512] *Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band*, ET Docket No. 13-49, First Report and Order, 29 FCC Rcd 4127, 4143, para. 54 (2014).

[513] Comcast Comments at 15-16 ("The FCC's history with Section 302 includes a number of analogous situations where the FCC cited Section 302 to justify rules or requirements ensuring the security of devices to avoid RF interference.").

160. Finally, consistent with our tentative conclusion in the *IoT Labeling NPRM*, we find that our section 302 authority enables us to rely on third parties in carrying out the implementation details of our Program.[514] As the Commission pointed out in the *NPRM*, section 302(e) of the Act authorizes the Commission to delegate equipment testing and certification to private laboratories, and the Commission already has relied in part on third parties in carrying out its equipment authorization rules that likewise implement section 302 of the Act.[515]

V. PROCEDURAL MATTERS

161. *Paperwork Reduction Act.* This document contains new and modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. It will be submitted to the Office of Management and Budget (OMB) for review under Section 3507(d) of the PRA. OMB, the general public, and other Federal agencies will be invited to comment on the new or modified information collection requirements contained in this proceeding. In addition, we note that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, see 44 U.S.C. 3506(c)(4), we previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees.

162. 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.

163. *Regulatory Flexibility Act*. Pursuant to the Regulatory Flexibility Act of 1980 (RFA), as amended,[516] the Commission's Final Regulatory Flexibility Analysis (FRFA) is set forth in Appendix B. The Commission's Office of the Secretary, Reference Information Center, will send a copy of this Report and Order, including the FRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).[517]

164. *Congressional Review Act*. [The Commission will submit this draft Report & Order to the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, for concurrence as to whether this rule is "major" or "non-major" under the Congressional Review Act, 5 U.S.C. § 804(2).] The Commission will send a copy of this [Report & Order, etc.] to Congress and the Government Accountability Office pursuant to 5 U.S.C. § 801(a)(1)(A).

165. *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,

[514] *IoT Labeling NPRM* at 25, para. 62. Although some commenters contest our section 302 authority as a general matter, no commenter contends that, insofar as section 302 of the Act does provide us authority, that authority would not be broad enough to allow us to rely on third parties as we do here.

[515] *Id*.

[516] *See* 5 U.S.C. § 603.

[517] *See id.* § 603(a).

and based on an open standard that is maintained by a standards organization.[518] This requirement is to be implemented "in accordance with guidance by the Director" of the OMB.[519] 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)."[520] A "data asset" is "a collection of data elements or data sets that may be grouped together,"[521] and "data" is "recorded information, regardless of form or the media on which the data is recorded."[522] 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.[523] In doing so, the Bureau shall take into account the extent to which such data assets are subject to disclosure under the FOIA.[524]

166. *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).

167. *Additional Information*. For further information regarding the Report and Order, please contact Drew Morin, Acting Chief, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau by email to drew.morin@fcc.gov; or James Zigouris, Attorney-Advisor, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-0697, or by email to james.zigouris@fcc.gov.

VI. ORDERING CLAUSES

168. Accordingly, IT IS ORDERED that pursuant to the authority contained in 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; the IoT Cybersecurity Improvement Act of 2020, 15 U.S.C. § 278g-3a to § 278g-3e; this *Report and Order* IS hereby ADOPTED.

169. IT IS FURTHER ORDERED that the amendments of the Commission's Rules as set forth in Appendix A are ADOPTED, effective 30 days after publication in the Federal Register, except for the amendments to 47 CFR §§ 8.207, 8.208, 8.209, 8.211, 8.213, 8.214, 8.216, 8.217, 8.218, 8.219, 8.220. The amendments to 47 CFR §§ 88.207, 8.208, 8.209, 8.211, 8.213, 8.214, 8.216, 8.217, 8.218, 8.219, 8.220, which may contain new or modified information collection requirements, will not become effective until OMB completes any review that the Public Safety and Homeland Security Bureau determines is required under the Paperwork Reduction Act. The Commission directs the Public Safety and Homeland Security Bureau to announce effective dates for these sections by publication in the Federal Register and

[518] Congress enacted the OPEN Government Data Act as Title II of the Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435 (2019), §§ 201-202. 44 U.S.C. § 3502(20), (22) (defining "open Government data asset" and "public data asset"); *id.* § 3506(b)(6)(B) (addressing public availability).

[519] 44 U.S.C. § 3506(b)(6)(B).

[520] 44 U.S.C. § 3502(22).

[521] *Id.* § 3502(17).

[522] *Id.* § 3502(16).

[523] OMB has not yet issued final guidance.

[524] *See, e.g.*, 5 U.S.C. § 552(b)(4), (6)-(7) (containing exemptions concerning confidential commercial information, personal privacy, and information compiled for law enforcement purposes, respectively).

by subsequent Public Notice.

170. IT IS FURTHER ORDERED that the Commission's Office of the Secretary, SHALL SEND a copy of this *Report and Order*, including the Final Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

171. IT IS FURTHER ORDERED that the Office of the Managing Director, Performance Program Management, SHALL SEND a copy of this *Report and Order* in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act, see 5 U.S.C. § 801(a)(1)(A).

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

APPENDIX A

Final Rules

The Federal Communications Commission amends Part 8 of Title 47 of the Code of Federal Regulations as follows:

PART 8 – INTERNET FREEDOM

Subchapter A of this part includes transparency for broadband internet access, while Subchapter B includes a labeling program for consumer IoT products.

1. The authority citation for part 8 is revised to read as follows:

AUTHORITY: 47 U.S.C. 154, 201(b), 257, 302, 303(r), and 1753.

2. Add §§ 8.901 – 8.1043 to read as follows:

I. General Provisions (§§ 8.201 – 8.206)

§ 8.201 Basis and purpose.

In order to elevate the nation's cybersecurity posture and provide consumers with assurances regarding their baseline cybersecurity, the Federal Communications Commission establishes a labeling program for Internet-connected (Internet of Things or IoT) products.

§ 8.202 Definitions.

(a) *Consumer IoT Products.* IoT products intended primarily for consumer use, rather than enterprise or industrial use. Consumer IoT Products exclude medical devices regulated by the U.S. Food and Drug Administration (FDA).

(b) *Cyber Trust Mark.* A visual indicator indicating a consumer IoT product complies with program requirements of the labeling program and the Commission's minimum cybersecurity requirements.

(c) *Cybersecurity Label Administrator (CLA).* An accredited third party entity that is recognized and authorized by the Commission to manage and administer the labeling program in accordance with the Commission's rules.

(d) *Lead Administrator.* A CLA selected from among Cybersecurity Label Administrators (CLAs) to be responsible for carrying out additional administrative responsibilities of the labeling program.

(e) *Cybersecurity Testing Laboratory (CyberLAB).* Accredited third party entities recognized and authorized by a CLA to assess consumer IoT products for compliance with requirements of the labeling program.

(f) *Intentional Radiator.* A device that intentionally generates and emits radiofrequency energy by radiation or induction.

(g) *Internet-Connected Device*. A device capable of connecting to the internet and exchanging data with other devices or centralized systems over the internet.

(h) *IoT Product*. An IoT device and any additional product components (e.g., backend, gateway, mobile app) that are necessary to use the IoT device beyond basic operational features.

(i) *IoT Device.*

(1) An Internet-connected device capable of intentionally emitting radiofrequency energy that has at least one transducer (sensor or actuator) for interacting directly with the

physical world, coupled with

(2) At least one network interface (e.g., Wi-Fi, Bluetooth) for interfacing with the digital world.

(j) *Product Components.* Components which generally fall into three main types per NISTIR 8425: specialty networking/gateway hardware (e.g., a hub within the system where the IoT device is used); companion application software (e.g., a mobile app for communicating with the IoT device); and backends (e.g., a cloud service, or multiple services, that may store and/or process data from the IoT device).

(k) *Labeling Program.* A voluntary program for consumer IoT products which allows a complying consumer IoT product to display an FCC IoT Label.

(l) *FCC IoT Label.* A binary label displayable with a consumer IoT product complying with program requirements of the Labeling Program, the binary label bearing the Cyber Trust Mark, and a scannable QR code which directs consumers to a registry containing further information on the complying consumer IoT product.

(m) *Registry.* Information presented to consumers about consumer IoT products that comply with the program requirements of the Labeling Program, the registry is publicly accessible through a link from the QR Code of the FCC IoT Label displayed with the complying consumer IoT product, and containing information about the complying consumer IoT product, manufacturer of the complying consumer IoT product, and other information as required by the Labeling Program.

§ 8.203 Prohibition on use of the FCC IoT Label on Products produced by listed sources.

(a) All consumer IoT products produced by sources listed in this subpart, are prohibited from obtaining use of the Label under this subpart. This includes:

(1) All communications equipment on the Covered List, as established pursuant to § 1.50002 of this chapter;

(2) All IoT Products containing IoT Devices or Product Components produced by entities listed in (3) or (4);

(3) IoT Devices or IoT Products produced by any entity, its affiliates, or subsidiaries identified on the Covered List as producing covered equipment, as established pursuant to § 1.50002 of this chapter; and

(4) IoT Devices or IoT Products produced by any entity, its affiliates, or subsidiaries identified on the Department of Commerce's Entity List, and/or the Department of Defense's List of Chinese Military Companies.

(5) Products produced by any entity owned or controlled by or affiliated with any person or entity that has been suspended or debarred from receiving federal procurements or financial awards, to include all entities and individuals published as ineligible for award on the General Service Administration's System for Award Management.

§ 8.203 Cybersecurity labeling authorization.

(a) Cybersecurity labeling authorization is an authorization issued by a Cybersecurity Label Administrator (CLA) and authorized under the authority of the Commission, which grants an applicant of a complying consumer IoT product to display the FCC IoT Label on the relevant packaging for the complying consumer product, based on compliance of the program requirements as determined by the CLA.

(b) Cybersecurity labeling authorization attaches to all units of the complying consumer IoT product subsequently marketed by the grantee that are identical (see § 8.204) to the sample determined to comply with the program requirements except for permissive changes or other variations authorized by the Commission.

§ 8.204 Identical defined.

As used in this subpart, the term identical means identical within the variation that can be expected to arise as a result of quantity production techniques.

§ 8.205 Responsible party.

In the case of a complying consumer IoT product that has been granted authorization to use the FCC IoT Label, the applicant to whom that grant of authorization is issued is responsible for continued compliance with the program requirements for continued use of the FCC IoT Label.

§ 8.206 Incorporation by reference.

Certain material is incorporated by reference into this part with the approval of the Director of the Federal Register in accordance with 5 U.S.C. 552(a) and 1 CFR part 51. All approved incorporation by reference (IBR) material is available for inspection at the FCC and at the National Archives and Records Administration (NARA). Contact the FCC at 1-888-225-5322. For information on the availability of this material at NARA, visit *www.archives.gov/federal-register/cfr/ibr-locations* or email fr.inspection@nara.gov. The material may be obtained from the following sources:

(a) International Electrotechnical Commission (IEC), IEC Central Office, 3, rue de Varembe, CH–1211 Geneva 20, Switzerland, Email: inmail@iec.ch, www.iec.ch.

(b) International Organization for Standardization (ISO), 1, ch. De la Voie-Creuse, CP 56, CH–1211, Geneva 20, Switzerland; www.iso.org; Tel.: + 41 22 749 01 11; Fax: + 41 22 733 34 30; email: central@iso.org. (ISO publications can also be purchased from the American National Standards Institute (ANSI) through its NSSN operation (www.nssn.org), at Customer Service, American National Standards Institute, 25 West 43rd Street, New York, NY 10036, telephone (212) 642–4900).

(1) ISO/IEC 17011:2017, "Conformity assessment—Requirements for accreditation bodies accrediting conformity assessment bodies," Second Edition, November 2017; IBR approved for §§ 8.216(e) and 8.217(b).

(2) ISO/IEC 17025:2017(E), "General requirements for the competence of testing and calibration laboratories," Third Edition, November 2017; IBR approved for §§ 8.216(a), (b), (e), 8.217(b), and 8.219(d).

(3) ISO/IEC 17065:2012(E), "Conformity assessment—Requirements for bodies certifying products, processes and services," First Edition, September 9, 2012; IBR approved for §§ 8.218(b), 8.219(b), (c), (d), (f), and (g).

II. Application Procedures for IoT Product Authorizations (§§ 8.207 – 8.211)

§ 8.207 Application requirements.

(a) An application to certify the consumer IoT product as being compliant with the Labeling Program shall be submitted in writing to a Cybersecurity Labeling Administrator (CLA) in the form and format prescribed by the Commission. Each application shall be accompanied by all information required by this subpart.

(b) The applicant shall provide to the CLA in the application all information that the CLA requires to determine compliance with the program requirements of the Labeling Program.

(1) The applicant shall provide a written and signed declaration to the CLA that all statements it makes in the application are true and correct to the best of its knowledge and belief.

(2) Each application, including amendments thereto, and related statements of fact and authorizations required by the Commission, shall be signed by the applicant or their authorized agent.

(3) The applicant shall provide an unsworn declaration under penalty of perjury that the consumer IoT product for which the applicant is applying for participation in the Labeling Program is not prohibited pursuant to § 8.203.

(4) If the identified listed sources under § 8.203 are modified after the date of the unsworn declaration required by paragraph (b)(3) of this section but prior to grant of authorization to use the FCC IoT Label, then the applicant shall provide a new unsworn declaration as required by paragraph (b)(3) of this section.

(5) The applicant shall designate an agent located in the United States for the purpose of accepting service of process on behalf of the applicant.

(i) The applicant shall provide a written attestation:

(A) Signed by both the applicant and its designated agent for service of process, if different from the applicant;

(B) Acknowledging the applicant's consent and the designated agent's obligation to accept service of process in the United States for matters related to the applicable product, and at the physical U.S. address and email address of its designated agent; and

(C) Acknowledging the applicant's acceptance of its obligation to maintain an agent for service of process in the United States for no less than one year after either the grantee has permanently terminated all marketing and importation of the applicable equipment within the U.S., or the conclusion of any Commission-related administrative or judicial proceeding involving the product, whichever is later.

(ii) An applicant located in the United States may designate itself as the agent for service of process.

(c) Technical test data submitted to the CLA shall be signed by the person who performed or supervised the tests. The person signing the test data shall attest to the accuracy of such data. The CLA may require the person signing the test data to submit a statement showing that they are qualified to make or supervise the required measurements.

(d) Signed, as used in this section, means an original handwritten signature; however, the Public Safety and Homeland Security Bureau may allow signature by any symbol executed or adopted by the applicant or CLA with the intent that such symbol be a signature, including symbols formed by computer-generated electronic impulses.

§ 8.208 Grant of Authorization to use FCC IoT Label.

(a) A CLA will grant authorization to use the FCC IoT Label if it finds from an examination of the application and supporting data, or other matter which it may officially notice, that the consumer IoT product complies with the program requirements. Once the program requirements are fully established, we direct the Public Safety and Homeland Security Bureau to update this rule accordingly.

(b) Grants will be made in writing showing the effective date of the grant.

(c) Cybersecurity certification shall not attach to any product, nor shall any use of the Cyber Trust Mark be deemed effective, until the application has been granted.

(d) Grants will be effective from the date of authorization.

(e) The grant shall identify the CLA granting the authorization and the Commission as the issuing authority.

(f) In cases of a dispute, the Commission will be the final arbiter.

§ 8.209 Dismissal of application.

(a) An application that is not in accordance with the provisions of this subpart may be dismissed.

(b) Any application, upon written request signed by the applicant or their agent, may be dismissed prior to a determination granting or denying the authorization requested.

(c) If an applicant is requested to submit additional documents or information and fails to submit the requested material within the specified time period, the application may be dismissed.

§ 8.210 Denial of application.

If the CLA is unable to make the findings specified in § 8.208(a), it will deny the application. Notification of the denial to the applicant will include a statement of the reasons for the denial.

§ 8.211 Review of CLA decisions.

(a) Any party aggrieved by an action taken by a CLA must first seek review from the CLA.

(b) A party aggrieved by an action taken by a CLA may, after seeking review by the CLA, seek review from the Commission.

(c) Filing deadlines.

(1) An aggrieved party seeking review of a CA decision by the CLA shall file such a request within sixty (60) days from the date the Administrator issues a decision.

(2) An aggrieved party seeking review of a CLA decision by the Commission shall file such a request within sixty (60) days from the date the CLA issues a decision on the party's request for review.

(3) In all cases of requests for review, the request for review shall be deemed filed on the postmark date. If the postmark date cannot be determined, the applicant must file a sworn affidavit stating the date that the request for review was mailed.

(4) Parties must adhere to the time periods for filing oppositions and replies set forth in 47 CFR § 1.45.

(d) Review by the Public Safety and Homeland Security Bureau or the Commission.

(1) Requests for review of CLA decisions that are submitted to the Federal Communications Commission shall be considered and acted upon by the Public Safety and Homeland Security Bureau; provided, however, that requests for review that raise novel questions of fact, law or policy shall be considered by the full Commission.

(2) An aggrieved party may seek review of a decision issued under delegated authority by the Public Safety and Homeland Security Bureau pursuant to the rules set forth in part 1 of this chapter.

(e) Standard of review.

(1) The Public Safety and Homeland Security Bureau shall conduct de novo review of request for review of decisions issued by the Administrator.

(2) The Federal Communications Commission shall conduct de novo review of requests for review of decisions by the Administrator that involve novel questions of fact, law, or policy; provided, however, that the Commission shall not conduct de novo review of decisions issued by the Public Safety and Homeland Security Bureau under delegated authority.

(f) Time periods for Commission review of CLA decisions.

(1) The Public Safety and Homeland Security Bureau shall, within ninety (90) days, take action in response to a request for review of a CLA decision that is properly before it. The Public Safety and Homeland Security Bureau may extend the time period for taking action on a request for review of a CLA decision for a period of up to ninety days. The Commission may also at any time, extend the time period for taking action of a request for review of a CLA decision pending before the Public Safety and Homeland Security Bureau.

(2) The Commission shall issue a written decision in response to a request for review of a CLA decision that involves novel questions of fact, law, or policy within ninety (90) days. The Commission may extend the time period for taking action on the request for review of a CLA decision. The Public Safety and Homeland Security Bureau also may extend action on a request for review of a CLA decision for a period of up to ninety days.

(g) While a party seeks review of a CLA decision, they are not authorized to use the FCC IoT Label until the Commission issues a final decision authorizing their use of the FCC IoT Label.

III. Authorization Conditions (§§ 8.212 - 8.217)

§ 8.212 Limitations on Grants to use the FCC IoT Label.

(a) A grant of authorization to use the FCC IoT Label remains effective until set aside, revoked or withdrawn, rescinded, surrendered, or a termination date is otherwise established by the Commission.

(b) No person shall, in any advertising matter, brochure, etc., use or make reference to the FCC IoT Label or the Cyber Trust Mark in a deceptive or misleading manner.

§ 8.213 IoT product defect and/or design change.

When a complaint is filed directly with the Commission or submitted to the Commission by the Lead Administrator concerning a consumer IoT product being non-compliant with the Labeling Program, and the Commission determines that the complaint is justified, the Commission may require the grantee to investigate such complaint and report the results of such investigation to the Commission within 20 days. The report shall also indicate what action if any has been taken or is proposed to be taken by the grantee to correct the defect, both in terms of future production and with reference to articles in the possession of users, sellers and distributors.

§ 8.214 Retention of records.

(a) For complying consumer IoT products granted authorization to use the FCC IoT Label, the grantee shall maintain the records listed as follows:

(1) A record of the original design and specifications and all changes that have been made to the complying consumer IoT product that may affect compliance with the standards and testing procedures of this subpart.

(2) A record of the procedures used for production inspection and testing to ensure conformance with the standards and testing procedures of this subpart.

(3) A record of the test results that demonstrate compliance with the appropriate regulations in this chapter.

(b) Records shall be retained for a two-year period after the marketing of the associated product has been permanently discontinued, or until the conclusion of an investigation or a proceeding if the grantee is officially notified that an investigation or any other administrative proceeding involving its product has been instituted.

(c) – (d) [Reserved]

§ 8.215 Termination of Authorization to use the FCC IoT Label.

(a) Grant of authorization to use the FCC IoT Label is automatically terminated by notice of the Bureau following submission of a report as specified in § 8.213 has not been adequately corrected:

(1) For false statements or representations made either in the application or in materials or response submitted in connection therewith or in records required to be kept by § 8.214.

(2) If upon subsequent inspection or operation it is determined that the consumer IoT product does not conform to the pertinent technical requirements or to the representations made in the original application.

(3) Because of conditions coming to the attention of the Commission which would warrant it in refusing to grant authorization to use the FCC IoT Label.

(b) [Reserved]

§ 8.216 *CyberLABs***.**

(a) A CyberLAB providing testing of products seeking a grant of authorization to use the FCC IoT Label shall be accredited by a recognized accreditation body which must attest that the CyberLAB has demonstrated:

(1) Technical expertise in cybersecurity testing and conformity assessment of IoT devices and products.

(2) Compliance with accreditation requirements based on the International Organization for Standardization/International Electrotechnical Commission International Standard ISO/IEC 17025, (incorporated by reference, see § 8.206).

(3) Knowledge of FCC rules and procedures associated with products compliance testing and cybersecurity certification.

(4) Necessary equipment, facilities, and personnel to conduct cybersecurity testing and conformity assessment of IoT devices and products.

(5) Documented procedures for conformity assessment.

(6) Implementation of controls to eliminate potential conflicts of interests, particularly with regard to commercially sensitive information.

(7) That the CyberLAB is not an organization, its affiliates, or subsidiaries identified by the listed sources of prohibition under § 8.203.

(8) Recognition afforded to a CyberLAB under the Labeling Program will be automatically terminated for entities that are subsequently placed on the Covered List, listed sources of prohibition under § 8.203, or of it, its affiliate, or subsidiary is owned or controlled by a foreign adversary country defined by the Department of Commerce in 15 CFR § 7.4.

(9) That it has certified the truth and accuracy of all information it has submitted to support its accreditation.

(b) Once accredited or recognized the CyberLAB would be periodically audited and reviewed to ensure they continue to comply with the requirements of the ISO/IEC 17025 standard.

(c) The Lead Administrator will maintain a list of accredited CyberLABs that it has recognized, and make publicly available the list of accredited CyberLAB. Inclusion of a CyberLAB on the accredited list does not constitute Commission endorsement of that facility. In order to be recognized and included on this list, the accrediting organization must submit the information listed below to the Lead Administrator:

(1) Laboratory name, location of test site(s), mailing address and contact information;

(2) Name of accrediting organization;

(3) Scope of laboratory accreditation;

(4) Date of expiration of accreditation;

(5) Designation number;

(6) FCC Registration Number (FRN);

(7) A statement as to whether or not the laboratory performs testing on a contract basis;

(8) For laboratories outside the United States, details of the arrangement under which the accreditation of the laboratory is recognized;

(9) Other information as requested by the Commission.

(d) [Reserved]

(e) A laboratory that has been accredited with a scope covering the measurements required for the types of IoT products that it will test shall be deemed competent to test and submit test data for IoT products subject to cybersecurity certification. Such a laboratory shall be accredited by the Public Safety and Homeland Security Bureau recognized accreditation organization based on the International Organization for Standardization/International Electrotechnical Commission International Standard ISO/IEC 17025, (incorporated by reference, see § 8.206). The organization accrediting the laboratory must be recognized by the Public Safety and Homeland Security Bureau to perform such accreditation based on International Standard ISO/IEC 17011 (incorporated by reference, see § 8.206). The frequency for reassessment of the test facility and the information that is required to be filed or retained by the testing party shall comply with the requirements established by the accrediting organization, but shall occur on an interval not to exceed two years.

§ 8.217 Recognition of CyberLAB accreditation bodies.

(a) A party wishing to become a laboratory accreditation body recognized by the Public Safety and Homeland Security Bureau (PSHSB) must submit a written request to the Chief of PSHSB requesting such recognition. PSHSB will make a determination based on the information provided in support of the request for recognition.

(b) Applicants shall provide the following information as evidence of their credentials and qualifications to perform accreditation of laboratories that test equipment to Commission requirements, consistent with the requirements of § 8.216(e). PSHSB may request additional information, or showings, as needed, to determine the applicant's credentials and qualifications.

(1) Successful completion of an ISO/IEC 17011 (incorporated by reference, see § 8.206) peer review, such as being a signatory to an accreditation agreement that is acceptable to the Commission.

(2) Experience with the accreditation of radio and telecommunications testing laboratories to ISO/IEC 17025 (incorporated by reference, see § 8.206).

(3) Accreditation personnel/assessors with specific technical experience on the Commission cybersecurity certification rules and requirements.

(4) Procedures and policies developed for the accreditation of testing laboratories for FCC cybersecurity certification programs.

IV. Cybersecurity Label Administrators (CLA or Label Administrators) (§§ 8.218 - 8.964)

§ 8.218 Approval/Recognition of Cybersecurity Label Administrators

(a) An accredited third party entity wishing to become a Cybersecurity Label Administrator (CLA) must file a written application with the Commission. The Commission may approve the written application for the accredited third party entity to be recognized and authorized by the Commission as a CLA to manage and administer the labeling program by meeting the requirements of paragraph (b) or (c) of this section. An accredited third party entity that is recognized and authorized by the Commission to manage and administer the labeling program in accordance with the Commission's rules.

(b) In the United States, CLAs must be accredited and designated by the National Institute of Standards and Technology (NIST) under its National Voluntary Conformity Assessment Evaluation (NVCASE) program, or other recognized programs based on ISO/IEC 17065 (incorporated by reference, see § 8.206) to comply with the Commission's qualification criteria for CLAs. NIST may, in accordance with its procedures, allow other appropriately qualified accrediting bodies to accredit CLAs. CLAs shall comply with the requirements in § 8.219.

§ 8.219 Requirements for CLAs.

(a) CLAs designated by the Commission, or designated by another authority recognized by the Commission, shall comply with the requirements of this section. Each entity seeking authority to act as a CLA must file an application with the Commission for consideration by PSHSB, which includes a description of its organization structure, an explanation of how it will avoid personal and organizational conflict when processing applications, a description of its processes for evaluating applications seeking authority to use the FCC IoT Label, and a demonstration of expertise that will be necessary to effectively serve as a CLA including, but not limited to, the criteria in paragraph (b)(2) of this section.

(b) ***Methodology for reviewing applications.***

(1) A CLA's methodology for reviewing applications shall be based on type testing as identified in ISO/IEC 17065 (incorporated by reference, *see* § 8.206).

(3) A CLA's grant of authorization to use the FCC IoT Label shall be based on the application with all the information specified in this part. The Label Administrator shall review the application to determine compliance with the Commission's requirements and shall issue a grant of product cybersecurity certification in accordance with § 8.207.

(c) ***Criteria for designation.***

(1) To be designated as a CLA under this section, an entity shall demonstrate cybersecurity expertise

and capabilities in addition to industry knowledge of IoT and IoT labeling requirements.

(2) The entity shall demonstrate expert knowledge of NIST's cybersecurity guidance, including but not limited to NIST's recommended criteria and labeling program approaches for cybersecurity labeling of consumer IoT products.

(3) The entity shall demonstrate expert knowledge of FCC rules and procedures associated with product compliance testing and certification.

(4) The entity shall demonstrate knowledge of Federal law and guidance governing the security and privacy of agency information systems.

(5) The entity shall demonstrate an ability to securely handle large volumes of information and demonstration of internal security practices.

(6) To expedite initial deployment of the FCC labeling program, the Commission will accept and conditionally approve applications from entities that meet the other FCC program requirements and commit to obtain accreditation pursuant to all the requirements associated with ISO/IEC 17065 with the appropriate scope within six (6) months of the effective date by the adopted standards and testing procedures. The entity must also demonstrate implementation of controls to eliminate actual or potential conflicts of interests (including both personal and organizational), particularly with regard to commercially sensitive information. The Bureau will finalize the entity's application upon receipt and demonstration of ISO/IEC 17065 accreditation with the appropriate scope.

(7) The entity is not owned or controlled by or affiliated with any entity identified on the Commission's Covered List, listed sources of prohibition under § 8.203, or of it, its affiliate, or subsidiary is owned or controlled by a foreign adversary country defined by the Department of Commerce in 15 CFR § 7.4.

(d) ***External resources.***

(1) In accordance with the provisions of ISO/IEC 17065 the evaluation of a product, or a portion thereof, may be performed by bodies that meet the applicable requirements of ISO/IEC 17025 in accordance with the applicable provisions of ISO/IEC 17065 for external resources (outsourcing) and other relevant standards. Evaluation is the selection of applicable requirements and the determination that those requirements are met. Evaluation may be performed using internal Label Administrator resources or external (outsourced) resources.

(2) A CLA shall not outsource review or decision activities.

(3) When external resources are used to provide the evaluation function, including the testing of products subject to labeling, the CLA shall be responsible for the evaluation and shall maintain appropriate oversight of the external resources used to ensure reliability of the evaluation. Such oversight shall include periodic audits of products that have been tested and other activities as required in ISO/IEC 17065 when a CLA uses external resources for evaluation.

(e) ***Commission Approves a CLA.***

(1) The Commission will approve as a CLA:

(i) Any entity in the United States that meets the qualification criteria and is accredited and designated by NIST or NIST's recognized accreditor as provided in § 8.960(b).

(ii) The Commission will not approve as a CLA any organization, its affiliates, or subsidiaries listed in the listed sources of prohibition under § 8.203.

(2) The Commission will withdraw its approval of a CLA if the CLA's designation or accreditation is withdrawn, if the Commission determines there is just cause for withdrawing the approval, or upon request of the CLA. The Commission will limit the scope of products that can be certified by a CLA if its accreditor limits the scope of its accreditation or if the Commission determines there is good cause to do so. The Commission will notify a CLA in writing of its intention to withdraw or limit the scope of the CLA's approval and provide at least 60 days for the CLA to respond.

(3) The Commission will notify a CLA in writing when it has concerns or evidence that the CLA is not carrying out its responsibilities under the Labeling Program in accordance with the Commission's rules and policies and request that it explain and correct any apparent deficiencies.

(4) The Public Safety and Homeland Security Bureau FCC IoT Label shall provide notice to the CLA that the Bureau proposes to terminate the CLA’s authority and provide the CLA a reasonable opportunity to respond (not more than 20 days) before reaching a decision on possible termination.

(5) If the Commission withdraws its recognition of a CLA, all grants issued by that CLA will remain valid unless specifically set aside or revoked by the Commission.

(6) A list of recognized CLAs will be published by the Commission.

(f) ***Scope of responsibility.***

(1) A CLA shall receive and evaluate applications and supporting data requesting authority to use the FCC IoT Label on the product subject to the application.

(2) A CLA shall grant authorization to use the FCC IoT Label with a complying consumer IoT product in accordance with the Commission's rules and policies.

(3) A CLA shall accept test data from any Commission-recognized accredited CyberLAB, subject to the requirements in ISO/IEC 17065 and shall not unnecessarily repeat tests.

(4) A CLA may establish and assess fees for processing applications and other Commission-required tasks.

(5) A CLA may only act on applications that it has received or which it has issued a certification authorizing use of the FCC IoT Label.

(6) A CLA shall dismiss an application that is not in accordance with the provisions of this subpart or when the applicant requests dismissal, and may dismiss an application if the applicant does not submit additional information or test samples requested by the CLA.

(7) Within 30 days of the date of grant of authority to use the FCC IoT Label, the CLA issuing the grant may set aside the grant upon the request of the applicant or non-compliance with program requirements. The CLA shall notify the applicant and the Commission when a grant is set aside. After 30 days of being set aside, the Commission may revoke the grant.

(8) A CLA shall ensure that manufacturers make all required information accessible by the IoT registry.

(9) A CLA shall participate in a consumer education campaign in coordination with the Lead Administrator.

(10) A CLA shall receive complaints alleging an IoT product does not support the cybersecurity criteria conveyed by the Cyber Trust Mark and refer these complaints to the Lead Administrator which will notify the Public Safety and Homeland Security Bureau.

(11) A CLA may not:

(i) Make policy, interpret unclear provisions of the statute or rules, or interpret the intent of Congress;

(ii) Grant a waiver of the rules; or

(iii) Take enforcement actions.

(12) All CLA actions are subject to Commission review.

(g) ***Post-market surveillance requirements.***

(1) In accordance with ISO/IEC 17065, a CLA shall perform appropriate post-market surveillance activities. These activities shall be based on type testing a certain number of samples of the total number of product types for which the CLA has certified use of the Label.

(3) PSHSB may request that a grantee of authority to use the FCC IoT Label submit a product sample directly to the CLA that evaluated the grantee's application as part of the post market surveillance. Any product samples requested by the Commission and tested by the CLA will be counted toward a minimum number of samples that the CLA must test to meet its post market surveillance requirements.

(4) A CLA may also request a grantee submit samples of products that the CLA has certified to use the FCC IoT Label directly to the CLA.

(5) If during post market surveillance of a complying consumer IoT product, a CLA determines that the product fails to comply with the technical regulations (or other FCC requirements) for that product, the CLA shall immediately notify the grantee and the Commission in writing of its findings. The grantee shall provide a report to the CLA describing the actions taken to correct the situation, as provided in § 8.215, and the CLA shall provide a report of these actions to the Commission within 30 days.

(6) CLAs shall submit periodic reports to the Commission of their post-market surveillance activities and findings in a format and by a date specified by the Commission.

§ 8.920 Requirements for the Lead Administrator.

(a) Establishing a Lead Administrator. If more than one qualified entity is selected by the Commission to be a CLA, the Commission will select a Lead Administrator.

(1) Interface with the Commission on behalf of the CLAs, including but not limited to submitting to

the Bureau all complaints alleging a product bearing the FCC IoT Label does not meet the requirements of the Commission's labeling program;

(2) Coordinate and moderate stakeholder meetings;

(3) Accept, review, and approve or deny applications from labs seeking recognition as a lab authorized to perform the conformity testing necessary to support an application for authority to affix the FCC IoT Label, and maintain a publicly available list of Lead Administrator-recognized labs and a list of labs that have lost their recognition;

(4) Within 90 days of election as Lead Administrator, the Lead Administrator will, in collaboration with stakeholders (e.g. cyber experts from industry, government, and academia):

(i) submit to the Bureau recommendations identifying and/or developing the technical standards and testing procedures for the Commission to consider with regard to at least one class of IoT products eligible for the IoT Labeling Program. The Bureau will evaluate the recommendations, subject to any required public notice and comment, incorporate them by reference into the Commission's rules;

(ii) submit to the Bureau finalized recommendations on how often a given class of IoT products must renew their request for authority to bear the FCC IoT Label, which may be dependent on the type of product, and that such a recommendation be submitted in connection with the relevant standards recommendations for an IoT product or class of IoT products; The Bureau will evaluate the recommendations, and if the Bureau approves of the recommendations, subject to any required public notice and comment, incorporate them by reference into the Commission's rules; and

(iii) submit to the Bureau recommendations on the design of the FCC IoT Label, including but not limited to labeling design and placement (e.g., size and white spaces, product packaging.) The Bureau will evaluate the recommendations, and if the Bureau approves of the recommendations, subject to any required public notice and comment, incorporate them by reference into the Commission's rules.

(5) Submit to the Commission reports on CLAs' post-market surveillance activities and findings in the format and by the date specified by Public Safety and Homeland Security Bureau;

(6) Develop in collaboration with stakeholders a consumer education campaign, submit the plan to the Public Safety and Homeland Security Bureau, and participate in consumer education;

(7) Receive complaints about the registry from consumers and coordinate with manufacturers to resolve any technical problems associated with consumers accessing the information in the registry;

(8) Facilitate coordination between CLAs; and

(9) Submit to the Commission any other reports upon request of the Commission or as required by Commission rule.

APPENDIX B

Final Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] an Initial Regulatory Flexibility Analysis (IRFA) was incorporated in the *Cybersecurity Labeling for Internet of Things* Notice of Proposed Rulemaking (*IoT Labeling NPRM*) released in August 2023.[2] The Federal Communications Commission (Commission) sought written public comment on the proposals in the *IoT Labeling NPRM*, including comment on the IRFA. No comments were filed addressing the IRFA. This Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.[3]

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

2. In today's *Report and Order* (*Order*), the Commission adopts a voluntary U.S. Cyber Trust Mark (Cyber Trust Mark or Mark) cybersecurity labeling program for Internet-connected consumer Internet of Things (IoT) products that will provide consumers with an easy-to-understand indicator of a product's relative cybersecurity and improve consumer confidence and understanding of IoT product cybersecurity. Consumer IoT products are susceptible to a wide range of security vulnerabilities that can be exploited by attackers to gain unauthorized access to the IoT product and its data. Providing customers with an easy-to-understand label indicating that an IoT product has satisfied baseline cybersecurity standards allows a consumer to understand the relative security risk that the IoT product may pose when making a purchase. We adopt an IoT Labeling Program focusing on IoT "products," which in accordance with the Commission's proposed adoption of the definition proposed in the *IoT Labeling NPRM* incorporates the National Institute of Standards and Technology (NIST) definition of an IoT product as an "IoT device and any additional product components (e.g., backend, gateway, mobile app) that are necessary to use the IoT device beyond basic operational features."[4] The record supports the Commission's adoption of a program focused on the IoT product rather than the individual device, because a label on the product addresses the full functionality of the device and the most relevant components the consumer expects to be secured when they buy a product. In addition to enabling consistency in the treatment of programmatic elements across the federal government, our adopted definition of IoT product will include the component pieces of a device posing cybersecurity risks. We focus the IoT Labeling Program on "consumer" IoT rather than "enterprise" IoT, as such an approach will provide value to consumers most efficiently and expediently, without added complexity from the enterprise environment. Medical devices regulated by the U.S. Food and Drug Administration (FDA), and devices that pose a risk to national security and public safety are excluded from the program. We also exclude wired products at this time because of the Commission's interest in keeping the scope of the IoT Labeling Program clear and manageable during its debut and because there is support in the record for wireless intentional radiators as most prevalent types of consumer IoT devices contemplated in the *IoT Labeling NPRM*.

3. We adopt standards and testing procedures based on the NIST framework for IoT, adopt the use of one or more Cybersecurity Label Administrators (Label Administrators or CLAs), overseen by the Commission to manage certain aspects of the program, and assign tasks and duties to that administrator to ensure timely rollout of the program. The Commission will select from among the CLA applicants one entity to be the Lead Administrator. The Lead Administrator will collaborate with stakeholders to, among other things, develop recommendations on the development or identification of the technical standards and testing procedures that must be met for an IoT product to be eligible to be authorized to use the Cyber

[1] 5 U.S.C. § 603. The RFA, 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).

[2] *Cybersecurity Labeling for Internet of Things*, PS Docket No. 23-239, FCC 23-65, Notice of Proposed Rulemaking (Aug. 10, 2023) *(IoT Labeling NPRM)*.

[3] 5 U.S.C. § 604.

[4] *See IoT Labeling NPRM* at 8, para. 13.

Trust Mark; make recommendations to the Commission about how often a given class of IoT products must renew their request for authority to bear the Mark; and recommendations on specific IoT label formatting. The Lead Administrator will submit each of these recommendations to the Chief of the Public Safety and Homeland Security Bureau (Bureau) for review and possible approval.

4. We adopt a two-step process that must be followed by a manufacturer seeking authority to use the Cyber Trust Mark. The manufacturer must:

1) Obtain conformance testing and a report demonstrating that the IoT product meets the program's standards and other FCC requirements necessary to be authorized to bear the Cyber Trust Mark. This testing may be provided by an accredited and FCC-recognized laboratory, which may include a Cybersecurity Testing Laboratory (CyberLAB), a manufacturer's in-house lab, or a lab operated by a Label Administrator; and
2) Submit an application to the Label Administrator of their choice, which will review the applications and supporting test report, and will authorize the applicant's use of the Cyber Trust Mark on that product if all program requirements have been met.

This process will ensure the label reliably reflects the security of the IoT product and secure consumer trust in the label. This structure implements controls to assure consumers that the IoT products bearing the Mark have undergone a meaningful procedure involving verification by disinterested parties and that the product meets the Commission's requirements to obtain authority to affix the Cyber Trust Mark to a product.

5. The Commission further adopts a binary label with layering due to its consumer-friendly nature and its potential to streamline purchasing decisions. The label will contain a QR Code with an embedded link that directs the consumer to a registry that will display information about the security of the product for the consumer. To determine how the registry should be structured to best meet the goals of the IoT Labeling Program as we adopt it today, we direct the Bureau to seek comment and consider, as part of a public process, the technical details involved with the operation of the registry. The Commission also tasks the Lead Administrator with fielding complaints about the registry from consumers and coordinating with manufacturers to resolve any technical problems associated with consumers accessing the information in the registry. We also address renewal of the label, enforcement considerations, international reciprocal recognition of the label, and stress the importance of consumer education to understand the limits and benefits of the label, rooted in a consumer education framework created by NIST. These elements ensure the label is accessible and easily understood by consumers. Adopting the voluntary IoT Labeling Program described above will further the Commission's objective to provide better information to consumers about the cybersecurity of the IoT products they use, and bolster the cybersecurity of the nationwide IoT ecosystem.

B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

6. There were no comments filed that specifically address the proposed rules and policies in the IRFA.

C. Response to Comments by the Chief Counsel for Advocacy of the Small Business Administration

7. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA, the Commission is required to respond to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration (SBA) and to provide a detailed statement of any change made to the proposed rules as a result of those comments.[5] The Chief Counsel did not file any comments in response to the proposed rules in this proceeding.

D. Description and Estimate of the Number of Small Entities to Which the Rules Will

[5] 5 U.S.C. § 604(a)(3).

Apply

8. The RFA directs agencies to provide a description of and, where feasible, an estimate of, the number of small entities that may be affected by the rules, adopted herein.[6] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[7] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[8] A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.[9]

9. *Small Businesses, Small Organizations, Small Governmental Jurisdictions.* Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe, at the outset, three broad groups of small entities that could be directly affected herein.[10] First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the Small Business Administration's (SBA) Office of Advocacy, in general a small business is an independent business having fewer than 500 employees.[11] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 33.2 million businesses.[12]

10. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field."[13] The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations.[14] Nationwide, for tax year 2020, there were approximately 447,689 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.[15]

[6] *Id.* § 604(a)(4).

[7] 5 U.S.C. § 601(6).

[8] 5 U.S.C. § 601(3) (incorporating by reference the definition of "small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[9] 15 U.S.C. § 632.

[10] *See* 5 U.S.C. § 601(3)-(6).

[11] *See* SBA, Office of Advocacy, "What's New With Small Business?, (2023)" https://advocacy.sba.gov/wp-content/uploads/2023/03/Whats-New-Infographic-March-2023-508c.pdf [https://perma.cc/Z824-JRBW].

[12] *Id*.

[13] *See* 5 U.S.C. § 601(4).

[14] The IRS benchmark is similar to the population of less than 50,000 benchmark in 5 U.S.C § 601(5) that is used to define a small governmental jurisdiction. Therefore, the IRS benchmark has been used to estimate the number of small organizations in this small entity description. S*ee* IRS, *Annual Electronic Filing Requirement for Small Exempt Organizations – Form 990-N (e-Postcard)* (Dec. 4, 2023), https://www.irs.gov/charities-non-profits/annual-electronic-filing-requirement-for-small-exempt-organizations-form-990-n-e-postcard [https://perma.cc/6QWK-CR8J]. We note that the IRS data does not provide information on whether a small exempt organization is independently owned and operated or dominant in its field.

[15] *See* IRS, *Exempt Organizations Business Master File Extract (EO BMF)* (Feb. 4, 2024), https://www.irs.gov/charities-non-profits/exempt-organizations-business-master-file-extract-eo-bmf [https://perma.cc/SXT4-U8C8]. The IRS Exempt Organization Business Master File (EO BMF) Extract provides information on all registered tax-exempt/non-profit organizations. The data utilized for purposes of this description was extracted from the IRS EO BMF data for businesses for the tax year 2020 with revenue less than or equal to

(continued….)

11. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[16] U.S. Census Bureau data from the 2017 Census of Governments[17] indicate there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States.[18] Of this number, there were 36,931 general purpose governments (county,[19] municipal, and town or township[20]) with populations of less than 50,000 and 12,040 special purpose governments—independent school districts[21] with enrollment populations of less than 50,000.[22] Accordingly, based on the 2017 U.S. Census of Governments data, we estimate that at least 48,971 entities fall into the category of "small governmental jurisdictions."[23]

12. *Radio Frequency Equipment Manufacturers (RF Manufacturers).* There are several analogous industries with an SBA small business size standard that are applicable to RF Manufacturers. These industries are Fixed Microwave Services, Other Communications Equipment Manufacturing, Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing. A description of these industries and the SBA small business size standards are detailed below.

$50,000 for Region 1-Northeast Area (58,577), Region 2-Mid-Atlantic and Great Lakes Areas (175,272), and Region 3-Gulf Coast and Pacific Coast Areas (213,840) that includes the continental U.S., Alaska, and Hawaii. This data does not include information for Puerto Rico.

[16] *See* 5 U.S.C. § 601(5).

[17] *See* 13 U.S.C. § 161. The Census of Governments survey is conducted every five (5) years compiling data for years ending with "2" and "7". *See also* U.S. Census Bureau, *Census of Governments, About* (Nov. 18, 2021), https://www.census.gov/programs-surveys/cog/about.html [https://perma.cc/E2FJ-TRXF].

[18] *See* U.S. Census Bureau, 2017 Census of Governments – Organization Table 2. Local Governments by Type and State: 2017 [CG1700ORG02], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html [https://perma.cc/ALG9-KB5A]. Local governmental jurisdictions are made up of general purpose governments (county, municipal and town or township) and special purpose governments (special districts and independent school districts). *See also* tbl.2. CG1700ORG02 Table Notes_Local Governments by Type and State_2017.

[19] *See id.* at tbl.5. County Governments by Population-Size Group and State: 2017 [CG1700ORG05], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html [https://perma.cc/ALG9-KB5A]. There were 2,105 county governments with populations less than 50,000. This category does not include subcounty (municipal and township) governments.

[20] *See id.* at tbl.6. Subcounty General-Purpose Governments by Population-Size Group and State: 2017 [CG1700ORG06], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html [https://perma.cc/ALG9-KB5A]. There were 18,729 municipal and 16,097 town and township governments with populations less than 50,000.

[21] *See id.* at tbl.10. Elementary and Secondary School Systems by Enrollment-Size Group and State: 2017 [CG1700ORG10], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html [https://perma.cc/ALG9-KB5A]. There were 12,040 independent school districts with enrollment populations less than 50,000. *See also* tbl.4. Special-Purpose Local Governments by State Census Years 1942 to 2017 [CG1700ORG04], CG1700ORG04 Table Notes_Special Purpose Local Governments by State_Census Years 1942 to 2017.

[22] While the special purpose governments category also includes local special district governments, the 2017 Census of Governments data does not provide data aggregated based on population size for the special purpose governments category. Therefore, only data from independent school districts is included in the special purpose governments category.

[23] This total is derived from the sum of the number of general purpose governments (county, municipal and town or township) with populations of less than 50,000 (36,931) and the number of special purpose governments - independent school districts with enrollment populations of less than 50,000 (12,040), from the 2017 Census of Governments - Organizations tbls. 5, 6 & 10.

13. *Fixed Microwave Services.* Fixed microwave services include common carrier,[24] private-operational fixed,[25] and broadcast auxiliary radio services.[26] They also include the Upper Microwave Flexible Use Service (UMFUS),[27] Millimeter Wave Service (70/80/90 GHz),[28] Local Multipoint Distribution Service (LMDS),[29] the Digital Electronic Message Service (DEMS),[30] 24 GHz Service,[31] Multiple Address Systems (MAS),[32] and Multichannel Video Distribution and Data Service (MVDDS),[33] where in some bands licensees can choose between common carrier and non-common carrier status.[34] Wireless Telecommunications Carriers (*except* Satellite)[35] is the closest industry with an SBA small business size standard applicable to these services. The SBA small size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[36] U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year.[37] Of this number, 2,837 firms employed fewer than 250 employees.[38] Thus, under the SBA size standard, the Commission estimates that a majority of fixed microwave service licensees can be considered small.

14. The Commission's small business size standards with respect to fixed microwave services involve eligibility for bidding credits and installment payments in the auction of licenses for the various frequency bands included in fixed microwave services. When bidding credits are adopted for the auction of licenses in fixed microwave services frequency bands, such credits may be available to several types of small businesses based on average gross revenues (small, very small, and entrepreneur) pursuant to the competitive bidding rules adopted in conjunction with the requirements for the auction and/or as identified in Part 101 of the Commission's rules for the specific fixed microwave services frequency

[24] *See* 47 CFR Part 101, Subparts C and I.

[25] *See id*. Subparts C and H.

[26] Auxiliary Microwave Service is governed by Part 74 of Title 47 of the Commission's Rules. *See* 47 CFR Part 74. Available to licensees of broadcast stations and to broadcast and cable network entities, broadcast auxiliary microwave stations are used for relaying broadcast television signals from the studio to the transmitter, or between two points such as a main studio and an auxiliary studio. The service also includes mobile TV pickups, which relay signals from a remote location back to the studio.

[27] *See* 47 CFR Part 30.

[28] *See* 47 CFR Part 101, Subpart Q.

[29] *See id*. Subpart L.

[30] *See id*. Subpart G.

[31] *See id*.

[32] *See id.* Subpart O.

[33] *See id*. Subpart P.

[34] *See* 47 CFR §§ 101.533, 101.1017.

[35] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers* (*except Satellite*)," https://www.census.gov/naics/?input=517312&year=2017&details=517312 [https://perma.cc/NBD5-UHZ9] (last visited Feb. 14, 2024).

[36] *See* 13 CFR § 121.201, NAICS Code 517312 (as of 10/1/22, NAICS Code 517112).

[37] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false [https://perma.cc/XKA9-98E9] (last visited Feb. 14, 2024).

[38] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

bands.[39]

15. In frequency bands where licenses were subject to auction, the Commission notes that as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Further, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. Additionally, since the Commission does not collect data on the number of employees for licensees providing these services, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard.

16. *Other Communications Equipment Manufacturing*. This industry comprises establishments primarily engaged in manufacturing communications equipment (except telephone apparatus, radio and television broadcast, and wireless communications equipment).[40] Examples of such manufacturing include fire detection and alarm systems manufacturing, Intercom systems and equipment manufacturing, and signals (e.g., highway, pedestrian, railway, traffic) manufacturing.[41] The SBA small business size standard for this industry classifies firms having 750 or fewer employees as small.[42] For this industry, U.S. Census Bureau data for 2017 shows that 321 firms operated for the entire year.[43] Of that number, 310 firms operated with fewer than 250 employees.[44] Based on this data, we conclude that the majority of Other Communications Equipment Manufacturers are small.

17. *Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing.* This industry comprises establishments primarily engaged in manufacturing radio and television broadcast and wireless communications equipment.[45] Examples of products made by these establishments are: transmitting and receiving antennas, cable television equipment, GPS equipment, pagers, cellular phones, mobile communications equipment, and radio and television studio and broadcasting equipment.[46] The SBA small business size standard for this industry classifies firms having 1,250 employees or less as small.[47] U.S. Census Bureau data for 2017 show that there were 656 firms in

[39] *See* 47 CFR §§ 101.538(a)(1)-(3), 101.1112(b)-(d), 101.1319(a)(1)-(2), and 101.1429(a)(1)-(3).

[40] *See* U.S. Census Bureau, *2017 NAICS Definitions, "334290 Other Communications Equipment Manufacturing,"* https://www.census.gov/naics/?input=334290&year=2017&details=334290 [https://perma.cc/D4JU-E6ZZ] (last visited Feb. 14, 2024).

[41] *Id.*

[42] *See* 13 CFR § 121.201, NAICS Code 334290.

[43] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 334290, https://data.census.gov/cedsci/table?y=2017&n=334290&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false [https://perma.cc/EB69-799P] (last visited Feb. 14, 2024).

[44] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[45] *See* U.S. Census Bureau, *2017 NAICS Definition*, *334220 Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing,* https://www.census.gov/naics/?input=334220&year=2017&details=334220 [https://perma.cc/2EMS-VMD9] (last visited Feb. 14, 2024).

[46] *Id.*

[47] *See* 13 CFR § 121.201, NAICS Code 334220.

this industry that operated for the entire year.[48] Of this number, 624 had fewer than 250 employees.[49] Based on this data, we conclude that a majority of manufacturers in this industry are small.

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

18. As described above, the Commission adopts 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. The IoT Labeling Program framework incorporates, and is consistent with, certain NIST guidelines and protocols as part of the Commission's recognition that public-private collaboration that leverages the expertise and existing frameworks of the federal government, industry, and other stakeholders is necessary for the success of its voluntary IoT Labeling Program. The Commission will be the IoT Labeling Program owner and retain ultimate control over the IoT Labeling Program, however, third-party administrators will carry out responsibilities such as management of day-to-day functions, and development of processes, standards, and testing to be approved by the Commission. In light of the work that remains to be done for administration and implementation of the IoT Labeling Program, the Commission is not in a position to quantify the costs for small entities or to determine whether it will be necessary for small entities to hire professionals to comply with the IoT Labeling Program.

19. 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 the Commission adopts in the *Order*. More specifically, small entities and other applicants are required to have their product tested by an accredited and FCC-recognized CyberLAB, Label Administrator Lab, or manufacturer's in-house lab; obtain a report of conformity and compliance from the testing lab; and submit an application for authority to use the Cyber Trust Mark to an FCC-recognized Label Administrator in accordance with procedures established by the Label Administrator. To ensure that IoT products approved for the use of the Cyber Trust Mark do not pose national security or public safety risks, small entities and other applicants seeking authorization to use to the Cyber Trust Mark are required to provide an unsworn declaration under penalty of perjury that as of the date they file their application that, (i) the product for which the applicant seeks to use the Mark through cybersecurity certification meets all the requirements of the IoT Labeling Program; (ii) the applicant is not identified on the Covered List, established pursuant to § 1.50002 of the of the Commission's rules, as an entity producing covered communications equipment; and (iii) the product is not produced by any entity, its affiliates, or subsidiaries identified on the Department of Commerce's Entity List, or the Department of Defense's List of Chinese Military Companies.

20. The *Order* adopts the NIST Core Baseline technical criteria presented in NISTIR 8425 as the foundation of the Commission's IoT Labeling Program as proposed in the *IoT Labeling NPRM*. Small entities and others seeking use of the Mark will be required to provide information on asset identification; product configuration; data protection; interface access control; software update; cybersecurity state awareness; and the IoT product development activities, on documentation, information and query reception, information dissemination, and product education and awareness for each product submission. To ensure their IoT products are eligible for continued use of the Cyber Trust Mark, small entities will need to keep the records necessary to demonstrate the products continue to comply with the IoT Labeling

[48] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 334220, https://data.census.gov/cedsci/table?y=2017&n=334220&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false [https://perma.cc/Q649-9AC4] (last visited Feb. 14, 2024).

[49] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

Program requirements. The Bureau has not yet adopted standards addressing how often an IoT product, or a class of IoT products, will need to be retested for continuing eligibility to display the Mark. While these standards have yet to be determined, maintaining records to demonstrate compliance with the minimum cybersecurity standards that are adopted will be necessary for small entities that elect to participate in the IoT Labeling Program. Additionally, small entities who participate in the IoT Labeling Program will be required to maintain appropriate records in the event their IoT product label authorization is subject to an audit.

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

21. The RFA requires an agency to provide, "a description of the steps the agency has taken to minimize the significant economic impact on small entities…including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected."[50]

22. The actions taken by the Commission in the *Order* were considered to be the least costly and minimally burdensome for small and other entities that choose to participate in the IoT Labeling Program. To serve the aims of the program, and 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 expressed in the IRFA for 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.

23. The Commission took a number of actions in the *Order* to minimize any significant economic impact on small entities and considered several alternatives. Specifically, the IoT Labeling Program is voluntary, so a small entity can engage in their own analysis to determine whether the benefits of participating in the program outweigh the costs of participating in the IoT Labeling Program with respect to any IoT products they manufacture. The Commission expects small entities that participate in the IoT Labeling Program like other entities will realize benefits from having the Cyber Trust Mark on their IoT product(s) such as product differentiation, increased consumer confidence, reduced risk of distributed denial-of-service (DDoS) and other types of cyber-attacks, and reduced cybersecurity incident related risks.

24. In the *Order*, the Commission has tasked the Lead Administrator with developing or identifying the standards to which every participant's IoT product must meet. Rather than formulating and adopting its own standards and testing procedures, the Commission opted to adopt standards based on recommendations made by the Lead Administrator in collaboration with industry stakeholders that will be able to leverage existing standards work in progress or completed, facilitating faster development of standards, and therefore facilitating a faster rollout of the IoT Labeling Program. Small entities will benefit from the Commission directive that the Lead Administrator use as a foundation for the IoT Labeling Program the technical criteria developed by NIST in the NISTIR 8425, Profile of the IoT Core Baseline for Consumer IoT Products, which provides flexibility that can be applied across all types of consumer IoT products. Small entities will also benefit from the limited scope of the IoT Labeling Program which is only applicable to consumer IoT products.

25. The Commission's decision to allow manufacturers seeking certification to use the Cyber Trust Mark the option to conduct in-house conformity testing for IoT products, provided the in-house labs meet the same accreditation and FCC-recognition requirements as CyberLABs, is a step that may benefit small entities. To the extent that a Cybersecurity Label Administrator also operates an in-house lab to

[50] 5 U.S.C. § 604(a)(6).

conduct conformity testing, the ability of small entities to use the Cybersecurity Label Administrator for both product testing and certification to use the Cyber Trust Mark may yield both time and costs saving for small entities. Also related to lab testing, the Commission considered but declined to require conformity testing labs to be physically located in the U.S., which provides more testing lab options for small and other entities. The Commission also considered but declined to allow self-attestation of conformity with testing requirements by applicants seeking the Cyber Trust Mark certification, citing support in the record of the certification of bogus products as Energy Star compliant in the Energy Star program when the program was "primarily a self-certification program relying on corporate honesty and industry self-policing to protect the integrity of the Energy Star label."[51]

26. The Commission anticipates that as the IoT Labeling Program becomes established in the minds of the consumer, small entities may benefit from recognition of the Cyber Trust Mark on their IoT products, and thus receive greater recognition in the market as a result of participating in the program. The Commission considered utilizing and adopted a single binary label as proposed in the *IoT Labeling NPRM* in part due to its simplicity to consumers, but a simple label benefits small businesses who want to place the label on their product as the small entity will not need to accommodate a more complex, and likely more costly, labeling regime on product packaging.

27. The Commission also considered arguments advocating against imposing unnecessarily rigid or burdensome requirements to participate in the IoT Labeling Program, in response to the renewal requirement proposal in the *IoT Labeling NPRM* that participants be required to file for renewal annually providing supporting documentation that their products continue to meet the IoT Labeling Program requirements.[52] Agreeing that different types of IoT products may require different renewal standards depending on their lifespan and level of risk, the Commission opted to task the Lead Administrator to collaborate with stakeholders and recommend a product-centered approach.[53] The Commission directed that the recommendation consider whether annual compliance report filings could be used for renewal purposes, and the recommendation balance the need to provide the industry with flexibility, while ensuring that consumers are provided up-to-date product information in a timely fashion to inform their purchasing decisions. The Commission sought to make the IoT Labeling Program sufficiently flexible for participants by taking achievable steps that preserve the IoT Labeling Program's integrity, while also making it accessible to as many small and other manufacturers as possible.

G. Report to Congress

28. The Commission will send a copy of the *Report and Order*, including this FRFA, in a report to Congress pursuant to the Congressional Review Act.[54] In addition, the Commission will send a copy of the *Report and Order*, including this FRFA, to the Chief Counsel for Advocacy of the SBA. A copy of the *Report and Order* and FRFA (or summaries thereof) will also be published in the *Federal Register*.[55]

[51] Government Accountability Office, Energy Star Program, Covert Testing Shows the Energy Star Program Certification Process Is Vulnerable to Fraud and Abuse, GAO-10-470 (2010), https://www.gao.gov/assets/files.gao.gov/assets/gao-10-470.pdf [https://perma.cc/9VB5-ZWTA].

[52] AHAM Comments 4.

[53] *Id.* at 4-5; Whirlpool Comments at 5; CTA Reply at 7; NAM Comments at 5; Kaiser Permanente Comments at 2; CCDS Comments at 5; CSA Comments at 19.

[54] 5 U.S.C. § 801(a)(1)(A).

[55] *Id.* § 604(b).