FEDERAL COMMUNICATIONS COMMISSION

47 CFR Subchapter A

[PSHSB: PS Docket No. 23–239; FR ID 210726]

Cybersecurity Labeling for Internet of Things

AGENCY: Federal Communications Commission.

ACTION: Final rule.

SUMMARY: In this document, the Federal Communications Commission (Commission or FCC) establishes a voluntary cybersecurity labeling program for wireless consumer Internet of Things, or IoT, products. The program will provide consumers with an easy-to-understand and quickly recognizable FCC IoT Label that includes the U.S. Cyber Trust Mark and a QR code linked to a dynamic, decentralized, publicly available registry of more detailed cybersecurity information. This program will help consumers make safer purchasing decisions, raise consumer confidence regarding the cybersecurity of the IoT products they buy, and encourage manufacturers to develop IoT products with security-by-design principles in mind.

DATES:

Effective date: This rule is effective August 29, 2024.

Incorporation by reference: The incorporation by reference of certain material listed in the rule is approved by the Director of the Federal Register as of August 29, 2024.

Compliance date: Compliance with 47 CFR 8.208, 8.209, 8.212, 8.214, 8.215, 8.217, 8.218, 8.219, 8.220, 8.221, and 8.222 will not be required until the Office of Management and Budget has completed review under the Paperwork Reduction Act. The Commission will publish a document in the **Federal Register** announcing that compliance date.

FOR FURTHER INFORMATION CONTACT: Zoe Li, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418–2490, or by email to *Zoe.Li@fcc.gov.*

For additional information concerning the Paperwork Reduction Act information collection requirements contained in this document, contact Nicole Ongele, Office of Managing Director, Performance and Program Management, 202–418–2991, or by email to *PRA@fcc.gov.*

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Report and Order, PS Docket No. 23–239, adopted March 14, 2024, and released March 15, 2024. The full text of this document is available by downloading the text from the Commission's website at: *https://docs.fcc.gov/public/attachments/FCC-24-26A1.pdf.* When the FCC Headquarters reopens to the public, the full text of this document will also be available for public inspection and copying during regular business hours in the FCC Reference Center, 45 L Street NE, Washington, DC 20554. To request this document in accessible formats for people with disabilities (*e.g.,* Braille, large print, electronica files, audio format, etc.) or to request reasonable accommodations (*e.g.,* accessible format documents, sign language interpreters, CART, etc.), send an email to *FCC504@fcc.gov* or call the FCC's Consumer and Government Affairs Bureau at (202) 418–0530 (voice), (202) 418–0432 (TTY).

Congressional Review Act: The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, concurs, that this rule is non-major under the Congressional Review Act, 5 U.S.C. 804(2). The Commission will send a copy of the Order to Congress and the Government Accountability Office pursuant to 5 U.S.C. 801(a)(1)(A).

Synopsis

1. With the 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 IoT products. 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 U.S. 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. The 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. In the 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.

3. Voluntary IoT Labeling Program. 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 Notice of Proposed Rulemaking (NPRM),* 88 FR 58211 (August 25, 2023), sought comment on whether the proposed IoT Labeling Program should be voluntary, 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.'' The record shows substantial support for a voluntary approach. The Custom Electronic Design & Installation Association (CEDIA) suggests that IoT Labeling Program must be voluntary ''for the program to gain momentum in the marketplace.'' AIM, Inc. (AIM) suggests that the voluntary aspect of the IoT Labeling Program ''will help drive adoption of the label by device producers.'' Further, commenters suggest that a voluntary program will ensure the broadest reach, most efficiency, and widest access to a diversity of IoT technologies. 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. Additionally, we acknowledge the view that ''consumer labeling is a difficult undertaking in any context,'' especially

in the evolving area of cybersecurity, and that the ''best approach is to start the Program with something achievable and effective.'' 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 distinguish products in the marketplace that meet minimum requirements and provide options to consumers.

4. We reject arguments that mandating participation in the IoT Labeling Program is necessary. While we recognize that a voluntary IoT Labeling Program may cause concern that smaller businesses with limited resources may choose not to participate, 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,'' 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.

5. In adopting the IoT Labeling Program with the parameters discussed in the *Order,* we are establishing a collaborative effort between the Federal Government and relevant stakeholders in industry and the private sector. We emphasize that the *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 the 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).

A. Eligible Devices or Products

6. The 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.

7. The record supports adopting an 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. In addition, we exclude from this program motor vehicles [1] and motor vehicle equipment (as defined in 49 U.S.C. 30102(8) given that the National Highway Traffic Safety Administration (NHTSA) ''has the authority to promulgate motor vehicle safety regulations on cybersecurity and has enforcement authority to secure recalls of motor vehicles and motor vehicle equipment with a safety-related defect, including one involving cybersecurity flaws.'' We also exclude from our IoT Labeling program any communications equipment on the Covered List that the Commission maintains pursuant to the Secure 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.

8. 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 National Institute of Standards and Technology (NIST) definition of ''IoT device'' that the Commission proposed in the IoT Labeling NPRM. Specifically, the IoT Labeling NPRM proposed defining an IoT device to include (1) an internet-connected device capable of intentionally emitting radio frequency (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. 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.'' The modified definition adopted in the Order 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. It should be noted that we direct the Label Administrator to collaborate with Cybersecurity Label Administrators (CLAs) and other stakeholders (*e.g.,* cyber experts from industry, government, and academia) as appropriate and recommend within 45 days of publication of updates or changes to NIST guidelines, or adoption by NIST of new guidelines, to the FCC any appropriate modifications to the Labeling Program standards and testing procedures to stay aligned with the NIST guidelines.

9. 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.'' 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].'' TIC Council Americas similarly ''agrees that 'internet-connected' should be included in the definition of IoT devices.'' 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.' '' 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.

10. We disagree with commenters who argue the Commission should adopt the NIST definition of a device without change. 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

[1] Motor Vehicle ''means a vehicle driven or drawn by mechanical power and manufactured primarily for use on public streets, roads, and highways, but does not include a vehicle operated only on a rail line.'' 49 U.S.C. 30102(7).

Americas, for example, supports adding ''internet-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.'' 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,'' with a concern that the device might become ''disconnected from the internet and, therefore, no longer be an 'IoT device.' '' 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.

11. 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. 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. 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, 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.

12. 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.'' 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 by traditional means.'' The Electronic Privacy Information Center (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. 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. 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.

13. Definition of IoT Products. We adopt the NIST definition of an ''IoT product.'' 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.'' 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.'' 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.'' 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.'' 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 the *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.[2] This view is supported by the record, with Consumer Technology Association (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.''

14. *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

[2] 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 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.

that it was important to ensure that the IoT Labeling Program ''would be sufficiently inclusive to be of value to consumers.'' 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.'' 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) ''including data communications links to components outside this scope but excluding those external components and any external third-party components that are outside the manufacturer's control'' 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.

15. There is significant support in the record for an IoT product focus for the IoT Labeling Program. 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.'' 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.'' 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).'' 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.'' 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.'' Further, focusing on IoT products aligns not only with the technical requirements of NISTIR 8425, but also ''emerging requirements in Europe and the UK [United Kingdom], such as the EU [European Union] [Cyber Resilience Act], and EU Directives on consumer protections EU 2019/770, 771.'' 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.

16. We disagree with Samsung, CTIA—The Wireless Association (CTIA), LG Electronics, and CTA, who advocate focusing on IoT devices instead of IoT products. Samsung and CTIA argue that cybersecurity standards for devices are more mature than standards for products, and CTA argues that applying the FCC IoT Label to products would be more complex than devices. 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.'' 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, 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.

17. 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. 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.

18. 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. We note, for example, that ITI recommends recognizing IoT security assessments from our international partners, such as IoT 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. 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.

19. 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.'' Additionally, as noted by UL Solutions, ''most IoT devices sold to consumers cannot be meaningfully used without additional components.'' 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; [2]

[2] To further clarify, nothing in this item prohibits manufacturers from allowing product owners from installing the software of their choice, from disabling security features, or from replacing or modifying components of a product, including the firmware and software. An IoT manufacturer cannot

Continued

however, where a manufacturer allows third-party apps, for example, to connect to and they allow that application to 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. Further, we agree with CTIA that if ''a [p]roduct [c]omponent also support[s] other IoT Products through alternative features and interfaces, these alternative features and interfaces may, through risk-assessment, be considered as separate from and not part of the IoT Product for purposes of authorization.'' 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,'' and that ''these additional components can introduce new or unique risks to the IoT product.'' 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.'' 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.'' The record is adamant that the ''Cyber Trust Mark must be trusted by consumers to be successful.'' 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.

20. 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.

21. Consumer IoT Products vs. Enterprise IoT Products. The IoT Labeling Program applies to the labeling of consumer IoT products that are intended for consumer use, 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.

22. 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 (CSA), among others. 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. Additionally, commenters highlight the differing security needs of consumer and enterprise products. 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.'' CSA also highlights that ''[e]nterprise device security approaches are often customized and vary based on the specific needs of the business.'' 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.

23. The International Speech and Communication Association (ISCA) supports including enterprise IoT, stating that a broader scope will ensure the IoT Labeling Program remains flexible to the extent that the boundary between consumer and enterprise IoT is blurring. Further, ISCA and Abhishek Bhattacharyya note that attackers have more to gain from targeting enterprise settings. While there are considerable threat vectors and vulnerabilities associated with all classes of IoT products,[3] 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. 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. 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.

24. Exclusion of Certain 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). 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. 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).'' These considerations persuade us to exclude FDA-regulated medical devices from our IoT Labeling Program, consistent with commenters' recommendations. In

be held responsible for the owner's decision to make such changes, just as a traditional product manufacturer cannot be responsible for the actions of a consumer who modifies the core mechanisms of a product and thereby risks rendering it unsafe. However, we reiterate that in order to be authorized to use the FCC IoT Label, manufacturers must meet the requirements of the program.

[3] 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.

addition, we exclude from this program motor vehicles and motor vehicle equipment given that the National Highway Traffic Safety Administration (NHTSA) ''has the authority to promulgate motor vehicle safety regulations on cybersecurity and has enforcement authority to secure recalls of motor vehicles and motor vehicle equipment with a safety-related defect, including one involving cybersecurity flaws.''

25. 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 Covered List maintained by the Commission pursuant to section 2 of the Secure and Trusted Communications Networks Act (STCNA); (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. 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. 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. 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, named on the Department of Defense's List of Chinese Military Companies, 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, 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 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.

26. With the exception of China's comments raising the same World Trade Organization (WTO) issue we rejected in the Report and Order applying the Covered List to the FCC equipment authorization program, the record overwhelmingly supports excluding from the IoT Labeling Program these products and devices produced by companies identified on the Covered List. 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, but also urge the Commission to restrict any equipment manufactured by companies on additional Federal restricted lists, including those otherwise banned from Federal procurement. Consumer Reports agrees with excluding systems that include components included on the Covered List or similar lists from the IoT Labeling Program. 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 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.

27. 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 a declaration under penalty of perjury that all of the following are true and correct:

(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, established pursuant to § 1.50002 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.

(vi) The applicant has taken every reasonable measure to create a securable product.

(vii) The applicant will, until the support period end date disclosed in the registry, diligently identify critical vulnerabilities in our products and promptly issue software updates correcting them, unless such updates are not reasonably needed to protect against security failures.

(viii) The applicant will not elsewhere disclaim or otherwise attempt to limit the substantive or procedural enforceability of this declaration or of any other representations and commitments made on the FCC IoT Label or made for purposes of acquiring or maintaining authorization to use it.

28. 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.

29. Wireless Consumer IoT Devices vs. Wired Consumer IoT Devices. The *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, 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. 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.

30. We acknowledge there is substantial support in the record for including wired IoT 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. 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.' '' TÜV SÜD also encourages the Commission to cover both wired and wireless devices within the scope of the IoT Labeling Program, and AIM emphasizes the importance of the security of both wired and wireless IoT to the cybersecurity ecosystem. 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. The Association of Home Appliance Manufacturers (AHAM) points out that both wired and wireless IoT are included in the NIST definition.

31. 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,'' 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.'' 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.'' 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.

B. Oversight and Management of the IoT Labeling Program

32. 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.

33. 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. 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. 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.'' 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.

34. 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 the CLAs and other stakeholders, to identify or develop, and recommend to the Commission for approval, the IoT specific standards and testing procedures, procedures for post-market surveillance, 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 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.'' 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.'' 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.

35. 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. In addition, several commenters addressed whether obtaining a valid equipment authorization should be a pre-requisite for obtaining the Cyber Trust Mark, or whether obtaining approval to use the Cyber Trust Mark would be required as a condition for applying for an equipment authorization. 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; however, our existing part 2 rules will continue to prohibit the marketing of a device that does not have a valid equipment authorization.

36. 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 the 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.

37. 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 are based on NIST standards and guidance, that will be submitted to PSHSB for consideration and approval, and, subject to any required public notice and comment, adopted into the Commission's rules. The standards and testing procedures developed or identified in collaboration with CLAs and other stakeholders and submitted by the Lead Administrator for consideration by the Commission will, in turn, be used by accredited [4] testing labs recognized by the Lead Administrator—whether CyberLABs,[5] a CLA-run lab, or a testing lab internal to a company (in-house testing lab) for product testing.

38. 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. 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.

39. 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. The record supports the Commission's adoption of a labeling program that is supported by CLAs.

[4] 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 §§ 8.217(e) and 8.218(b).

[5] 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 below. 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.

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. 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.'' 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.'' 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.''

40. 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.

41. 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 testing against widely accepted cybersecurity guidelines (*e.g.,* NIST guidelines) or proprietary product profiles based on the NIST criteria. 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.

42. 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. 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.

43. 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,[6] 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 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; 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;

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; and

iv. submit to the Bureau recommendations with regard to updates to the registry including whether the registry should be in additional languages, and if so, to recommend specific languages for inclusion;

v. 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, whether to include

[6] 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.

the product support end date and other security and privacy information on the label.) 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. The Lead Administrator shall, in collaboration with CLAs and other stakeholders (*e.g.,* cyber experts from industry, government, and academia) as appropriate recommend within 45 days of publication of updates or changes to NIST guidelines, or adoption by NIST of new guidelines, to the FCC any appropriate modifications to the Labeling Program standards and testing procedures to stay aligned with the NIST guidelines;

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

g. develop in collaboration with stakeholders a consumer education campaign, submit the plan to the PSHSB, and participate in consumer education;

h. 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;

i. facilitate coordination between CLAs; and

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

44. 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 and submit periodic reports to the Lead Administrator of their 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.[7]

45. 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. CTA supports utilizing CLAs to conduct program operations. The Cybersecurity Coalition and Kaiser Permanente also support utilizing CLAs for managing the day-to-day operations of the IoT Labeling Program. 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.'' 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.'' CSA and CTIA further recommend adopting the IoT Labeling NPRM's proposal that a third-party administrator evaluate, accredit, or recognize the CyberLABs, and CSA also ''recommends that the Commission hire a third-party administrator to operate the IoT Registry.'' Finally, ioXt Alliance recommends that third-party administrators should also ''vet companies and products during the certification process'' 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.''

46. 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 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.

47. In addition to its role as a CLA, the Lead Administrator must collaborate with CLAs and other 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, adoption into its rules. Adopting standards through consensus is supported by the record in this proceeding.[8] 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.'' ITI also notes that using industry-led, consensus standards will also limit the likelihood of legal challenges. UL Standards & Engagement

[7] 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 through 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.

[8] 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.

agrees that the FCC should use a ''voluntary consensus-based standards development process'' to create and update standards for the IoT Labeling Program. 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) and CTIA's cybersecurity certification program for IoT devices.'' 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,'' including the C2 Consensus document, which provides guidance to the public and private sectors on IoT devices security. 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 provide for the swift development and implementation of the IoT Labeling Program.

48. 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.'' 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. The Lead Administrator should evaluate and leverage existing work for efficiency and speed to market where appropriate in making its recommendations to the Commission.

49. 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. 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, 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.

50. Selecting CLAs. Each entity seeking authority to act as a CLA must file an application with the Commission for consideration by PSHSB,[9] 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.

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 with the appropriate scope.[10] 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.[11]

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, and the Department of Defense's List of Chinese Military Companies.

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

[9] This approach necessitates a mechanism for the Commission to recognize administrators, and we accordingly adopt a rule doing so. *See* 47 CFR 8.219. 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).

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

[11] 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.

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.

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 the Order;

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

e. a proposed consumer education campaign; and

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

51. 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.'' 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.'' 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 assurances to the American public that products meet 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.

52. NCTA—The Internet & Television Association (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.'' Further, ioXt Alliance recommends that the Commission ''establish rules to ensure CyberLABs are not subject to undue influence by foreign adversaries.'' 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 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, 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 the Office of International Affairs (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.

53. We decline to require that a CLA be a non-profit. 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. 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. 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. 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.

54. 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 PSHSB, to determine if a CLA's authority is to be terminated in the latter circumstance, and to terminate such authorization.[12] PSHSB, may identify such CLA deficiencies itself or receive notice from other entities, including other agencies, consumers,

[12] 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.

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.

55. 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 the *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. 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 the *Order.* We also delegate to PSHSB authority to adopt additional criteria and administrative procedures necessary to efficiently select one or more independent, non-governmental entities, to act as CLA(s) and Lead Administrator. The Lead Administrator must provide equitable recommendations to the Commission to encourage the broadest possible participation of CLAs within the parameters of the FCC's rules.[13] We also delegate to PSHSB authority to adopt additional criteria and procedures in the event the Lead Administrator must be replaced or chooses to withdraw from its responsibilities.[14] 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.

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

56. The Commission envisioned the role of CyberLABs as assessing IoT devices or products for compliance against IoT security standards, once developed. 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. 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.

57. 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. 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. 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.[15]

58. The Order agrees 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. 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

[13] We also agree with CTA in highlighting the importance of PSHSB's involvement in matters where the Lead Administrator and CLAs may share vested interests.

[14] We recognize the potential raised by ioXt Alliance for anticompetitive preferences in recommendations made to the Bureau if a CLA is chosen as Lead Administrator.

[15] 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 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.

integrity of the IoT Labeling Program. The Order also agrees 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.''

59. We agree with CSA's argument that the Commission should adopt a model where CyberLABs must be ISO/IEC 17025 accredited. 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. 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 (*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, and we agree.

60. 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. 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. 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.

61. 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 is to be applied. 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 in the Order, 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.

62. 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.'' 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. The Cybersecurity Coalition urges the Commission to allow for in-house testing. 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. 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.

63. 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.[16] As explained by the American Association for Laboratory Accreditation (A2LA), ''[a]ccreditation 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.'' 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.

64. 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.

[16] This approach necessitates a mechanism for the Commission to recognize lab accreditation bodies, and we accordingly adopt a rule doing so. *See* 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. 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.

65. 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.

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

67. 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.'' Further, ioXt Alliance recommends that the Commission ''establish rules to ensure CyberLABs are not subject to undue influence by foreign adversaries.'' 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, 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. 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. 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.

68. The Order notes that Garmin advocates even stricter measures on the testing labs, suggesting that the labs be ''located in the U.S.'' 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.'' 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.'' 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.

69. 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 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.[17] 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.

70. *Fees.* To fulfill their role, as envisioned by the *IoT Labeling NPRM,* we authorize CyberLABs to charge reasonable fees to conduct the tasks adopted in the Order. The *IoT Labeling NPRM* proposed a fee calculation methodology adopted by the Commission in the *2020 Application Fee Report and Order,* 86 FR 15026 (March 19, 2021), and sought comment on whether any oversight is needed by the Commission over such charges. 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

[17] 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.

the charges. We recognize the Cybersecurity Coalition's comments that high fees would deter participation in the IoT Labeling Program. We anticipate that there will be multiple CyberLABs authorized through the approach adopted in the Order, 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 (NAM) 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.'' 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.

D. Two-Step Process for Obtaining Authority To Use the FCC IoT Label

71. 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 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.

72. 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.

73. 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), and submitted to a third-party for verification of compliance with the Commission's program requirements. Others argue the Commission should accept a declaration of conformity or self-certification, 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. 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.

74. 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. 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 a Supplier's Declaration of Conformity (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.'' 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.

75. 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 process. The Commission recognizes the view of Keysight, the National Electronic Manufacturers Association (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. However, the Commission agrees with A2LA, which urges caution with self-attestations of conformity ''due to the bias inherent in self-declaration.'' 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,'' 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. 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.''

76. 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.

77. 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.

78. 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-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.[18] 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.

[18] 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* 47 CFR 8.208(i), (k). 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).

79. 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. 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. 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. 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. We outline the application process to use the FCC IoT Label below.

80. 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.

81. 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 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.

82. 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.

83. 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, 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. 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. We anticipate that there will be multiple administrators authorized through the approach adopted in the Order, 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.[19] 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.

84. 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.

85. 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 45 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 45 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.

E. Consumer IoT Product Cybersecurity Criteria and Standards

86. Technical Criteria for Consumer IoT Products. 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.

87. 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 [NIST], under NISTIR 8425.'' 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.

88. 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. CSA also supports adoption of the NIST Core Baseline but urges the Commission to refrain from developing its own standards for testing. 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, 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 . . .'' Garmin encourages the Commission to consider ETSI 303 645 standards, 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. These commenters did not oppose referencing the NIST criteria.

89. We agree with Infineon, Consumer Reports, and NCTA and adopt NISTIR 8425 as the basis for the Commission's IoT Labeling Program. 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 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). The following is the list of

[19] 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 the Order to be an exhaustive list of the shared costs we expect to be shared among CLAs as a whole.

the NIST IoT product capability criteria, NIST's brief description of each, and the NIST-identified cybersecurity utility for each:

(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-todate 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 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:

(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.

90. Consumer IoT Product Standards. 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). 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.'' 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.'' 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. . . ..''

91. We reject CTIA's recommendation that the Commission refrain from adopting specific standards and solely rely on the NIST criteria. 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.'' 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.

92. 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.'' 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.'' 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 quickly create its definitions and guidelines.'' 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.''

93. 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. 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.

94. 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.''

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

95. We adopt the IoT Labeling NPRM's proposal to implement a single binary label with layering. 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.''

96. 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. Similarly, as LG Electronics points out, ''[l]ike the ENERGY STAR program, 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. 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.'' 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.'' Another commenter suggests a multi-tiered label that would have different colors depending on the length of time the product is supported. 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. 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. We also recognize that some international regimes, such as Singapore, use a multi-tiered label.

97. 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.'' 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 necessary to meet the NIST baseline criteria in different contexts. 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.

98. 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.'' Power Tool Institute, Inc. concurs that ''[p]lacing a QR Code on the packaging is preferable to placing it on the device.'' Notable pros of using a QR Code are providing ''consumers with detailed information about a device or product,'' enhancing the program's objective by providing real-time updates. 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. 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.

99. 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. The Lead Administrator and stakeholders should also examine whether the label design should include the date the manufacturer will stop supporting the product as well as whether including other security and privacy information (*e.g.,* sensor data collection) on the label would be useful to consumers. In addition, the Lead Administrator should address the use of the FCC IoT Label in store displays and advertising.[20] 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 American National Standards Institute (ANSI)-accredited standards program. 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.'' 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. 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. The Cyber Trust Mark may only be used as directed by part 8, notwithstanding 47 CFR 2.935 or any other rule.

G. Registry

100. 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

[20] 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. 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.

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. There is robust support for the development of a publicly-accessible registry. We agree with NCTA that ''the IoT Registry is foundational to the value and utility of the Cyber Trust Mark Program.'' In the following paragraphs, we establish general parameters for registry information.

101. 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 that is secure by design. 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. 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.

102. 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. 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.'' CTIA further proposes that we should allow each manufacturer to establish their own mechanisms for conveying this information to consumers. However, we acknowledge ioXt Alliance's concern that a completely manufacturer-driven approach could lead to inconsistencies, inaccuracies, or other difficulties for the consumer. 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 information from the manufacture and display it to the consumer in a simple, uniform way:

- Product Name;
- Manufacturer name;
- Date product received authorization (*i.e.,* cybersecurity certification) to affix the label and current status of the authorization (if applicable);
- Name and contact information of the CLA that authorized use of the FCC IoT Label;
- Name of the lab that conducted the conformity testing;
- Instructions on how to change the default password (specifically state if the default password cannot be changed);
- Information (or link) for additional information on how to configure the device securely;
- Information as to whether software updates and patches are automatic and how to access security updates/patches if they are not automatic;
- The date until which the entity promises to diligently identify critical vulnerabilities in the product and promptly issue software updates correcting them, unless such an update is not reasonably needed to protect against cybersecurity failures (*i.e.,* the minimum support period); alternatively, a statement that the device is unsupported and that the purchaser should not rely on the manufacturer to release security updates;
- Disclosure of whether the manufacturer maintains a Hardware Bill of Materials (HBOM) and/or a Software Bill of Materials (SBOM);[21] and
- Additional data elements that the Bureau determines are necessary pursuant to the delegated authority discussed below.

103. 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'' and include in the registry information that is key to making a purchasing decision, without overwhelming the consumer. 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. 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. The Cybersecurity Coalition likewise expresses concern over the complexity of the proposed registry. 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.'' We believe that a registry containing simple, easy to understand information will be most helpful to a consumer making a purchasing decision, but also see the value in allowing manufacturers to include a second registry page (following the consumer-focused page) to enable manufacturers to provide additional technical details designed for researchers, enterprise purchasers, and other expert consumers of the label. Focusing only on the most critical information will further facilitate the speedy establishment of the IoT Labeling Program and the registry itself.

104. 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. 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. We recognize the value of ensuring the registry information is accessible to everyone, including those whose primary language is not English. Accordingly, we direct the Lead Administrator to recommend to the Bureau whether the registry should be in additional languages and if so, to recommend the specific languages for inclusion. We delegate authority to the Bureau to consider and adopt requirements in this regard upon review

[21] In addition to the declaration, the SBOM and HBOM will be made available upon request by the Commission, CyberLAB, and/or CLA.

of these recommendations. As the Association of Home Appliance Manufacturers points out, the location of the product's manufacture is redundant with existing legal requirements. 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, but we direct the Label Administrator to consider whether to recommend including the product support end date on labels for certain products, or category of products.

105. 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. 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 and HBOM 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. 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,'' but this is not what we require here. Requiring participating manufacturers to disclose only the maintenance of an SBOM and HBOM, rather than the contents therein, indicates an added level of software and hardware security while also protecting potentially sensitive information. Further, while we agree with CTA that a searchable registry would have value for the public, 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 NPRM. 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 in the Order 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.

106. 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.'' 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. The UK research did conclude, however, that continued manufacturer support was important to survey participants. Consumer Reports suggested an expiration date, if present, should be tied to an end-of-support date rather than a renewal date. 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 and end date for the 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. To ensure that information about this support period remains accurate, and to encourage manufacturers to support their products for longer periods, manufacturers shall be able to extend the support period in the registry through a mechanism to be determined by the Lead Administrator, but which should be expeditious and require no further disclosures.

107. 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. 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. 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, such as the manufacturer's access control protections (*e.g.,* information about passwords, multi-factor authentication), whether or not the data is encrypted while in motion and at rest (including in the home, app, and cloud), patch policies and security or privacy information are necessary, and if so, what should they be.

108. We disagree with commenters, such as LG Electronics, who suggest that manufacturers should have discretion over whether to include additional privacy and/or security information through a QR Code, URL, or other scannable mechanism insofar as it would require additional information in the registry. 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. 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. 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.

109. 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. 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. We agree that, given the structure of the registry as we adopt in the Order, the Lead Administrator is in the best position to interface with manufacturers to ensure the smooth operation of the registry.

110. 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 in the Order, 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, establishing the structure of the registry; 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; whether to require the manufacturer to list the product sensors, what data is collected, if the data is shared with third parties, or security or privacy issues and if data should be replicated; 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 in the Order. The Bureau should consider how to reduce burdens on manufacturers in supporting the decentralized registry. 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 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.

H. Continuing Obligations of Entities Authorized To Use the FCC IoT Label

111. 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 the Connected Consumer Device Security Council (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.

112. 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. Consumer Reports and TÜV SÜD agree that annual renewal is appropriate. AHAM feels that an annual renewal application as the Commission proposed was unnecessary, or at minimum ''unnecessarily rigid.'' 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. Similarly, more durable IoT products (such as smart appliances) may need to be renewed less frequently. NAM argues that annual renewals are unnecessary for products that pose a limited risk. Kaiser Permanente believes higher-risk devices should be updated annually, and otherwise renewal should occur every three years. 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. CSA suggests limiting the need for annual testing, but suggests some kind of annual reporting should be required. We observe that other certifying bodies, such as ioXt Alliance, require annual renewal for products they certify and allow incentives for early renewal. 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.

113. 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 renewal process, as we agree with Kaiser Permanente that renewal fees must not be unduly burdensome or cost-prohibitive. 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.

I. Audits, Post-Market Surveillance, and Enforcement

114. 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 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.

115. We find support in the record that the ''Mark must be trusted by consumers to be successful'' and ''to gain consumer confidence and incentivize cybersecurity, the label must be backed by a robust enforcement program.'' 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,'' and take up its recommendation of independent, post-market audits accordingly. 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. Whirlpool states that surveillance ''should include random auditing . . . as well as sampling of some established percentage on a regular basis of certified products/devices.'' The American Association for Laboratory Accreditation supports adopting the product surveillance standards established for Telecommunication Certification Bodies (TCBs) and in the EPA's ENERGY STAR program. 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. 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. We agree that random audits, in addition to regular post-market surveillance will best serve to maintain consumer confidence in the Cyber Trust Mark.[22]

116. 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, 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.

117. We believe it is appropriate for the Lead Administrator, in collaboration with the CLAs and other stakeholders, to identify or develop, and recommend to the Commission for approval, the post market surveillance activities and procedures that CLAs will use for performing post-market surveillance. The recommendations should include 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.[23] We delegate authority to the Bureau to review the recommendations and, subject to any required public notice and comment, incorporate post market procedures into the Commission's rules. 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 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.

118. 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). The IoT Labeling NPRM asked whether the IoT Labeling Program should adopt a similar process. 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'' and '' to address any discovered non-conformance as long as the manufacturer is acting in good faith.'' Here, we adopt a cure period of 20 days, which is in line with the ENERGY STAR program.

119. 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. 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. We delegate to the Bureau to consider whether such requirements should follow from termination of authority.

120. 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. Administrative remedies may include, but are not limited to, show cause orders, forfeitures, consent decrees, cease and desist orders, and penalties. 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,[24] and legal

[22] 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* 47 CFR 8.215. 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).

[23] 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.

[24] 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

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

121. 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 cybersecurity standards. While several commenters support Commission preemption of state laws, as well as adoption of liability protections for devices approved to display the Cyber Trust Mark, 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. 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. 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.

misleading manner. *See* 47 CFR 8.213(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).

J. International Reciprocal Recognition of the Cyber Trust Mark

122. We note the robust record highlighting the immense value to manufacturers of IoT products in international harmonization of cybersecurity standards. 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.'' 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.

123. We recognize several other countries already have an established national cyber IoT labeling program, including Singapore, Finland, and Germany. The record cites to these programs and highlights their features for consideration in developing the IoT Labeling Program. 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). We note that other commenters have also recommended use of the ETSI EN 303 645 standards. Further, the record provides Finland's IoT labeling database as an example for developing our IoT registry. Several other countries have government activity around IoT devices or products. For example, Canada has a cybersecurity certification program for small and medium-sized organizations. 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.

124. 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 adhere to specific requirements. 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. Further, Japan has committed to work with the U.S. to ''ensure interoperability'' of its IoT labeling scheme currently under development.

125. We fully recognize the importance of ensuring international recognition of the IoT Labeling Program and reciprocity considerations underlie our decisions in the Order. 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.

K. Consumer Education

126. 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 due to its general applicability to an IoT label and in light of support from the record. 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. 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, the Commission will coordinate as needed with relevant agencies, such as the Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation

(FBI), as well as the FTC, the Consumer Product Safety Commission (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.

127. We agree with CEDIA that consumer education will have a significant impact on meeting the IoT Labeling Program's goals. 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, 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. 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.'' 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.

128. 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. 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;

(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.

129. 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, and thus envision a Lead Administrator-led, multiple stakeholder engagement that puts NIST's recommendations into practice.

130. NIST has conducted research into the consumer perspective on the loss of manufacturer support in IoT products. 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. 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. We agree with Consumer Reports that educating consumers about the meaning of support periods is an important aspect of consumer education. 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.

131. 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, 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, but do not propose how to conduct outreach consistent with the Federal outreach concerns articulated in the *IoT Labeling NPRM.* 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. We agree with CTA that Federal consumer education efforts do not preclude independent communication and outreach programs. For example, the National Retail Foundation indicated their willingness to support consumer education efforts. While Everything Set, Inc. is concerned that outsized private sector involvement in consumer education might hurt the campaign's credibility, 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.

L. Cost/Benefit Analysis

132. 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.

133. 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. 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 the 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 cybersecurity risk. 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. We note that this calculation only focuses on one segment of the IoT market, which may underestimate the time savings induced by the *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. 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 Labeling Program to incur these benefits in the first year of the program, and every year thereafter. Nationwide, the Cyber Trust Mark would result in a minimum of $60 million in time savings annually.[25]

134. 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. 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. 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. 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.

135. 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 Labeling Program and from increased company goodwill and reduced risks related to cybersecurity incidents. 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. 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. 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.

136. 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. We do further emphasize this as a benefit that is likely to have significant impacts on firms in a wide range of industries.

137. 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 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.

138. 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. This provides some indication that manufacturers perceive the benefits of participating in the IoT Labeling Program as outweighing the costs. We understand

[25] $60 million = (15,000,000*$16*(15/60)) is the estimated value for 15 minutes of time savings nationwide.

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.

139. 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. 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.[26] 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. 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. 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. 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 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.

140. 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.

I. Legal Authority

141. 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. 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. 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.

142. Some commenters question our authority under section 302 to establish an IoT Labeling Program. The U.S. Chamber of Commerce cautions the Commission to not ''overinterpret its harmful interference authority'' under sections 302(a) and 333. 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 in the Order does not fall within the scope of section 302(a) or any other section of the Communications Act. 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.

143. We agree with Comcast that Congress intended section 302 to be flexible enough ''to address novel issues not yet on the legislative radar[.]'' 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).'' 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. 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.

144. 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.'' 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.

145. 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:

> 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

[26] 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. The registry, as adopted, does not include these features and therefore would not incur the costs to develop and maintain them.

systems will not be subject to malfunction due to [radio frequency interference].

146. 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. Examples given by Congress were home burglar alarms, security systems, automatic garage door openers, record turntables, and sound systems. 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. 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.

147. 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). 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. 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.'' 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. Under the circumstances here, we thus find it ''reasonable'' for our IoT Labeling Program to rely on the full package 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. 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. Thus, although we do not rely on additional provisions beyond section 302 as authority for the voluntary IoT Labeling Program we adopt in the Order, they inform our understanding of what regulatory approach to implementing section 302(a) is reasonable under these circumstances.[27]

148. Comcast also cites the legislative history of section 302(a) in support of our authority to establish an IoT Labeling Program. 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. Congress instead adopted the current language: ''reasonable regulations . . . consistent with the public interest, convenience, and necessity.'' 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.'' 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.'' 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.

149. 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. 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'' and actions to secure unlicensed national information infrastructure devices are sufficiently analogous to this proceeding as to be supported by our section 302 authority.

150. 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. 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.

II. Incorporation by Reference

151. These final rules include regulatory text that is incorporated by reference. In accordance with requirements of 1 CFR 51.5, the Commission describes the incorporated materials here. These final rules are incorporating by reference the following ISO/IEC standards: ISO/IEC 17011:2017(E), *Conformity assessment—Requirements for accreditation bodies accrediting conformity assessment bodies,* Second Edition, November 2017, ISO/IEC 17025:2017(E), *General requirements for the competence of testing and calibration laboratories,* Third Edition, November 2017, and ISO/IEC 17065:2012(E), *Conformity assessment—Requirements for bodies certifying products, processes and services,* First Edition, 2012–09–15, which establish international standards requirements for accreditation bodies accrediting conformity assessment bodies; general requirements for testing and calibration laboratories; and conformity assessment requirements for certifying products, processes, and services; respectively. Copies of these standards are available for purchase 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.

III. Procedural Matters

152. *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

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

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.

153. In this 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 in the Order. 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.

154. *Regulatory Flexibility Act Analysis.* A Final Regulatory Flexibility Act (FRFA) Analysis for the final rules adopted in the Order was prepared and can be found as Exhibit B of the FCC's Report and Order, FCC 24–26, adopted March 15, 2024, at this link: *https://docs.fcc.gov/public/attachments/FCC-24-26A1.pdf.*

155. *OPEN Government Data Act.* The OPEN Government Data Act requires agencies to make ''public data assets'' available under an open license and as ''open Government data assets,'' *i.e.,* in machine-readable, open format, unencumbered by use restrictions other than intellectual property rights, and based on an open standard that is maintained by a standards organization. This requirement is to be implemented ''in accordance with guidance by the Director'' of the OMB. The term ''public data asset'' means ''a data asset, or part thereof, maintained by the Federal Government that has been, or may be, released to the public, including any data asset, or part thereof, subject to disclosure under the Freedom of Information Act (FOIA).'' A ''data asset'' is ''a collection of data elements or data sets that may be grouped together,'' and ''data'' is ''recorded information, regardless of form or the media on which the data is recorded.'' We delegate authority, including the authority to adopt rules, to the Bureau, in consultation with the agency's Chief Data Officer and after seeking public comment to the extent it deems appropriate, to determine whether to make publicly available any data assets maintained or created by the Commission within the meaning of the OPEN Government Act pursuant to the rules adopted herein, and if so, to determine when and to what extent such information should be made publicly available. Such data assets may include assets maintained by a CLA or other third party, to the extent the Commission's control or direction over those assets may bring them within the scope of the OPEN Government Act, as interpreted in the light of guidance to be issued by OMB.[28] In doing so, the Bureau shall take into account the extent to which such data assets are subject to disclosure under the FOIA.

156. *People with Disabilities.* To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an email to *fcc504@fcc.gov* or call the Consumer & Governmental Affairs Bureau at 202–418–0530 (voice).

IV. Ordering Clauses

157. 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 through 278g–3e; the Report and Order *is* hereby *adopted.*

158. **It is further ordered** that the Office of the Managing Director, Performance Program Management, SHALL SEND a copy of the *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).

[28] OMB has not yet issued final guidance.

List of Subjects in 47 CFR Part 8

Communications, Consumer protection, Cybersecurity, Electronic products, Incorporation by reference, internet, Labeling, Product testing and certification, Telecommunications.

Federal Communications Commission

Marlene Dortch,

Secretary.

Final Rules

For the reasons discussed in the preamble, the Federal Communications Commission amends 47 CFR subchapter A as follows:

■ 1. Under the authority of 47 U.S.C. 151, 152, 153, 154(i)–(j), 160, 163, 201, 202, 206, 207, 208, 209, 214, 215, 216, 217, 218, 219, 220, 230, 251, 254, 256, 257, 301, 303, 304, 307, 309, 310, 312, 316, 332, 403, 501, 503, 522, 1302, revise the heading for subchapter A to read as follows:

Subchapter A—General

PART 8—SAFEGUARDING AND SECURING THE INTERNET

■ 2. The authority citation for part 8 continues to read as follows:

Authority: 47 U.S.C. 151, 152, 153, 154, 163, 201, 202, 206, 207, 208, 209, 216, 217, 257, 301, 302a, 303, 304, 307, 309, 312, 316, 332, 403, 501, 503, 522, 1302, 1753.

■ 3. Revise the heading for part 8 to read as set forth above.

§§ 8.1, 8.2, 8.3, and 8.6 [Designated as Subpart A]

■ 4. Designate §§ 8.1, 8.2, 8.3, and 8.6 as subpart A.

■ 5. Add a heading for newly designated subpart A to read as follows:

Subpart A—Protections for internet Openness

■ 6. Add subpart B to read as follows:

Subpart B—Cybersecurity Labeling Program for IoT Products

Sec.

Subpart B—Cybersecurity Labeling Program for IoT Products

§ 8.201 Incorporation by reference.

Certain material is incorporated by reference into this subpart 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 Federal Communications Commission (FCC or Commission) and at the National Archives and Records Administration (NARA). Contact the FCC at the address indicated in 47 CFR 0.401(a), phone: (202) 418–0270. 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 International Electrotechnical Commission (IEC), IEC Central Office, 3, rue de Varembe, CH–1211 Geneva 20, Switzerland, Email: *inmail@iec.ch, www.iec.ch.*

(a) ISO/IEC 17011:2017(E), *Conformity assessment—Requirements for accreditation bodies accrediting conformity assessment bodies,* Second Edition, November 2017; IBR approved for § 8.217.

(b) ISO/IEC 17025:2017(E), *General requirements for the competence of testing and calibration laboratories,* Third Edition, November 2017; IBR approved for §§ 8.217; 8.220.

(c) ISO/IEC 17065:2012(E), *Conformity assessment—Requirements for bodies certifying products, processes and services,* First Edition, 2012–09–15; IBR approved for § 8.220.

Note 1 to § 8.201: The standards listed in this section are co-published with the 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.*

Note 2 to § 8.201: 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.

§ 8.202 Basis and purpose.

In order to elevate the Nation's cybersecurity posture and provide consumers with assurances regarding their baseline cybersecurity, thereby addressing risks of harmful radiofrequency interference to and from consumer internet-connected (Internet of Things or IoT) products the Federal Communications Commission establishes a labeling program for consumer IoT products.

§ 8.203 Definitions.

(a) *Affiliate.* For purposes of this subpart and the IoT labeling program, an *affiliate* is defined as a person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another person. For purposes of this subpart, the term *own* means to own an equity interest (or the equivalent thereof) of more than 10 percent.

(b) *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) and excludes motor vehicles and motor vehicle equipment regulated by the National Highway Traffic Safety Administration (NHTSA).

(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 in this subpart.

(d) *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.

(e) *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 in this subpart.

(f) *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 that directs consumers to a registry containing further information on the complying consumer IoT product.

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

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

(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) *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, including data communications links to components outside this scope but excluding those external components and any external third-party components that are outside the manufacturer's control.

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

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

(m) *Product components.* Hardware devices, plus supporting components that 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). Should a product component also support other IoT products through alternative features and interfaces, these alternative features and interfaces may, through risk-assessment, be considered as separate from and not part of the IoT product for purposes of authorization.

(n) *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.

§ 8.204 Prohibition on use of the FCC IoT Label on products produced by listed sources.

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

(a) All communications equipment on the Covered List, as established pursuant to 47 CFR 1.50002;

(b) All IoT products containing IoT devices or product components produced by entities listed in paragraph (c) or (d) of this section;

(c) 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 47 CFR 1.50002;

(d) IoT devices or IoT products produced by any entity, its affiliates, or subsidiaries identified on the Department of Commerce's Entity List, 15 CFR part 744, supplement no. 4, and/or the Department of Defense's List of Chinese Military Companies, 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 (Pub. L. 116–283), Tranche 2 (2022), *https://media.defense.gov/2022/Oct/05/2003091659/-1/-1/0/1260H%20COMPANIES.PDF*. and

(e) 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.

§ 8.205 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 with 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 § 8.206) to the sample determined to comply with the program requirements except for permissive changes or other variations authorized by the Commission.

§ 8.206 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.

§ 8.207 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 cybersecurity labeling authorization is issued is responsible for continued compliance with the program requirements for continued use of the FCC IoT Label.

§ 8.208 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.

(c) The applicant will provide a declaration under penalty of perjury that all of the following are true and correct:

(1) 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.

(2) The applicant is not identified as an entity producing covered communications equipment on the Covered List, established pursuant to 47 CFR 1.50002.

(3) The product is not comprised of ''covered'' equipment on the Covered List.

(4) The product is not produced by any entity, its affiliates, or subsidiaries identified on the Department of Commerce's Entity List, 15 CFR part 744, supplement no. 4, and/or the Department of Defense's List of Chinese Military Companies, 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 (Pub. L. 116–283), Tranche 2 (2022), *https://media.defense.gov/2022/Oct/05/2003091659/-1/-1/0/1260H%20COMPANIES.PDF;* and

(5) 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 as described in § 8.204.

(6) The applicant has taken every reasonable measure to create a securable product.

(7) The applicant will, until the support period end date disclosed in the registry, diligently identify critical vulnerabilities in our products and promptly issue software updates correcting them, unless such updates are not reasonably needed to protect against security failures.

(8) The applicant will not elsewhere disclaim or otherwise attempt to limit the substantive or procedural enforceability of this declaration or of any other representations and commitments made on the FCC IoT Label or made for purposes of acquiring or maintaining authorization to use it.

(d) 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.

(e) 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.

(f) The applicant declares the product is reasonably secure and will be updated through minimum support period for the product and the end date of the support period must be disclosed.

(g) The applicant shall declare 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 § 8.204.

(h) If the identified listed sources under § 8.204 are modified after the date of the declaration required by paragraph (c) of this section but prior to grant of authorization to use the FCC IoT Label, then the applicant shall provide a new declaration as required by paragraph (c).

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

(1) The applicant shall provide a written attestation:

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

(ii) 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

(iii) 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.

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

(j) 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.

(k) *Signed,* as used in this section, means an original handwritten signature or 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.

§ 8.209 Grant of authorization to use FCC IoT Label.

(a) A CLA will grant cybersecurity labeling authorization 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.

(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.

§ 8.210 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.

§ 8.211 Denial of application.

If the CLA is unable to make the findings specified in § 8.209(a), it will deny the application. Notification of the denial to the applicant will include a statement of the reasons for the denial.

§ 8.212 Review of CLA decisions.

(a) *Seeking review from a CLA.* Any party aggrieved by an action taken by a CLA must first seek review from the CLA. The CLA should respond to appeals of their decisions in a timely manner and within 10 business days of receipt of a request for review.

(b) *Seeking review from the Commission.* 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 CLA decision by the CLA shall submit such a request within sixty (60) days from the date the CLA issues a decision. Such request shall be deemed submitted when received by the CLA.

(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. 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 47 CFR part 1.

(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 CLA.

(2) The Federal Communications Commission shall 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 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 forty-five (45) 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 forty-five (45) 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) *No authorization pending CLA review.* 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.

§ 8.213 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.

§ 8.214 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 or other party 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.

§ 8.215 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.

§ 8.216 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 § 8.214 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 § 8.215.

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

(4) Because the grantee or affiliate has been listed as described in § 8.204.

(b) [Reserved]

§ 8.217 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 ISO/IEC 17025 (incorporated by reference, see § 8.201).

(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 § 8.204.

(8) 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 will 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 verify that the CyberLAB is not listed in any of the lists in § 8.204.

(d) 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. 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 § 8.204, 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.

(e) In order to be recognized and included on the list in paragraph (d) of this section, the accrediting organization must submit the information in paragraphs (e)(1) through (9) of this section 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; and

(9) Other information as requested by the Commission.

(f) 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 a Public Safety and Homeland Security Bureau-recognized accreditation organization based on ISO/IEC 17025. The organization accrediting the laboratory must be recognized by the Public Safety and Homeland Security Bureau to perform such accreditation based on ISO/IEC 17011 (incorporated by reference, see § 8.201). 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.

§ 8.218 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 or Bureau) 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 information in paragraphs (b)(1) through (4) of this section as evidence of their credentials and qualifications to perform accreditation of laboratories that test equipment to Commission requirements, consistent with the requirements of § 8.217(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 peer review, such as being a signatory to an accreditation agreement that is acceptable to the Commission.

(2) Experience with the accreditation of conformity assessment testing laboratories to ISO/IEC 17025.

(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.

§ 8.219 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) of this section. An accredited third-party entity is recognized and authorized by the Commission to manage and administer the labeling program in accordance with the Commission's rules in this subpart.

(b) In the United States, the Commission, in accordance with its procedures, allows qualified accrediting bodies to accredit CLAs based on ISO/IEC 17065 and other qualification criteria. CLAs shall comply with the requirements in § 8.220.

§ 8.220 Requirements for CLAs.

(a) *In general.* 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 (c) 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 § 8.201).

(2) 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 CLA shall review the application to determine compliance with the Commission's requirements in this subpart and shall issue a grant of product cybersecurity certification in accordance with § 8.208.

(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 National Institute of Standards and Technology's (NIST) 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 demonstrate internal security practices.

(6) To expedite initial deployment of the FCC labeling program, the Commission will accept and conditionally approve applications from entities seeking to be designated as a CLA provided they 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 and otherwise meet the FCC's IoT Labeling Program requirements. 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 § 8.204, 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.

(8) The entity must demonstrate it has implemented 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.

(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). Evaluation is the selection of applicable requirements and the determination that those requirements are met. Evaluation may be performed using internal CLA 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 requirements of this section.

(ii) The Commission will not approve as a CLA any organization, its affiliates, or subsidiaries listed in the listed sources of prohibition under § 8.204.

(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 in this subpart and policies and request that it explain and correct any apparent deficiencies.

(4) The Public Safety and Homeland Security Bureau 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 in this subpart and policies.

(3) A CLA shall accept test data from any Lead Administrator-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) A CLA shall ensure that manufacturers make all required information accessible to the IoT registry.

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

(9) A CLA shall receive complaints alleging a product bearing the FCC IoT Label 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.

(10) 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 in this subpart; or

(iii) Take enforcement actions.

(11) 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.

(2) 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.

(3) 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.

(4) 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 § 8.216, and the CLA shall provide a report of these actions to the Commission within 30 days.

(5) 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.

§ 8.221 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. The Lead Administrator shall:

(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 with CLAs 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 the CLAs and 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 in this subpart;

(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. 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 in this subpart;

(iii) Submit to the Bureau a recommendation on procedures for post market surveillance by the CLAs. 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 in this subpart;

(iv) Make recommendations to the Bureau with regard to updates to the registry including whether the registry should be in additional languages, and if so, to recommend specific languages for inclusion; and

(v) 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) and whether to include the product support end date on labels for certain products or category of 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 in this subpart;

(5) Within 45 days of publication of updates or changes to NIST guidelines, or adoption by NIST of new guidelines,

recommend in collaboration with CLAs and other stakeholders any appropriate modifications to the labeling program standards and testing procedures to stay aligned with the NIST guidelines;

(6) 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;

(7) 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;

(8) 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;

(9) Facilitate coordination between CLAs; and

(10) Submit to the Commission any other reports upon request of the Commission or as required by Commission rules in this subpart.

(b) *Criteria for designation.* 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:

(1) Their previous experience in IoT cybersecurity;

(2) What role, if any, they have played in IoT labeling;

(3) Their capacity to execute the Lead Administrator duties;

(4) How they would engage and collaborate with stakeholders to identify or develop the Bureau recommendations;

(5) A proposed consumer education campaign; and

(6) Additional information the applicant believes demonstrates why they should be the Lead Administrator.

§ 8.222 Establishment of an IoT Registry.

(a) A grantee of authority to use the FCC IoT Label shall provide information about the complying consumer IoT product to the public. Information supplied by grantees shall be made available in a dynamic, decentralized, publicly accessible registry through a common Application Programming Interface (API) that is secure by design.

(b) A grantee of authority to use the FCC IoT Label shall publish the following information through the common API in the Registry:

(1) Product Name;

(2) Manufacturer name;

(3) Date the 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 (specifically state if the default password cannot 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) The date until which the entity promises to diligently identify critical vulnerabilities in the product and promptly issue software updates correcting them, unless such an update is not reasonably needed to protect against cybersecurity failures (*i.e.,* the minimum support period); alternatively, a statement that the device is unsupported and that the purchaser should not rely on the manufacturer to release security updates;

(10) Disclosure of whether the manufacturer maintains a Hardware Bill of Materials (HBOM) and/or a Software Bill of Materials (SBOM); and

(11) Additional data elements that the Bureau deems necessary.

[FR Doc. 2024–14148 Filed 7–29–24; 8:45 am]

BILLING CODE 6712–01–P