This document is scheduled to be published in the Federal Register on 2026-11-23 and available online at **https://www.federalregister.gov/d/2026-23812**, and on **https://govinfo.gov**

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 8

[PS Docket No. 23-239, DA 26-1162; FR ID 377778]

Cybersecurity Labeling for Internet of Things

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: In this document, the Public Safety and Homeland Security Bureau (Bureau) of the Federal Communications Commission (Commission or FCC) seeks comment on recommendations for the U.S. Cyber Trust Mark (USCTM) program, a voluntary cybersecurity labeling program for wireless consumer Internet of Things (IoT) products. The Bureau seeks comment on the design and placement of the FCC IoT Label, display of product registry information, certification renewal, post-market surveillance, and procedures for complaints, noncompliant products, and program administrators that withdraw or whose authority is terminated. These actions would support the establishment and effective administration of the USCTM program and provide consumers with accessible cybersecurity information about certified IoT products.

DATES: Comments are due on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**; reply comments are due on or before **[INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

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

- *Electronic Filers:* Comments may be filed electronically using the internet by accessing the ECFS: https://www.fcc.gov/ecfs.

- *Paper Filers:* Parties who choose to file by paper must file an original and one copy of each filing.
    - Filings can be sent by hand or messenger delivery, by commercial courier, or by the U.S. Postal Service. All filings must be addressed to the Secretary, Federal Communications Commission.
    - Hand-delivered or messenger-delivered paper filings for the Commission's Secretary are accepted between 8:00 a.m. and 4:00 p.m. by the FCC's mailing contractor at 9050 Junction Drive, Annapolis Junction, MD 20701. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.
    - Commercial courier deliveries (any deliveries not by the U.S. Postal Service) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
    - Filings sent by U.S. Postal Service First-Class Mail, Priority Mail, and Priority Mail Express must be sent to 45 L Street NE, Washington, DC 20554.
- *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.

Confidential Treatment. Parties wishing to file materials with a claim of confidentiality should follow the procedures set forth in § 0.459 of the Commission's rules. Casual claims of confidentiality are not accepted. Confidential submissions may not be filed via ECFS but rather should be filed with the Secretary's Office following the procedures set forth in 47 CFR 0.459. Redacted versions of confidential submissions may be filed via ECFS. Parties are advised that the FCC looks with disfavor on claims of confidentiality for entire documents. When a claim of confidentiality is made, a public, redacted version of the document should also be filed.

FOR FURTHER INFORMATION CONTACT: Tara B. Shostek, Attorney Advisor, (202) 418-8130, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau at CyberTrustMark@fcc.gov.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's document (*Public Notice*) in PS Docket No. 23-239, DA 26-1162, released on October 27, 2026. The full text of this document is available at the following Internet address: https://docs.fcc.gov/public/attachments/DA-26-1162A1.docx.

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

Paperwork Reduction Act Analysis. This document may contain proposed new or modified information collections. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and the Office of Management and Budget (OMB) to comment on any information collections contained in this document, as required by the Paperwork Reduction Act of 1995, 44 U.S.C. 3501-3521. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, 44 U.S.C. 3506(c)(4), the Commission seeks specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.

Ex Parte Rules – Permit but Disclose. This proceeding shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules. 47 CFR 1.1200 *et seq*. Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation

was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with rule 1.1206(b). In proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (e.g., .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

SYNOPSIS

USCTM LABEL REQUIREMENTS

The Lead Administrator's *Label Standard Cover Letter* introduces and describes the reasoning behind certain recommendations contained in the *Label Standard*, which provides stakeholder recommendations to inform the FCC IoT Label requirements for USCTM-certified products. In general, the *Label Standard* recommends definitions for key terms relevant to the label requirements, "General Requirements for Display" (including physical label design and dimensions and displaying the label online, in a catalog, via display collateral, and in product documentation), "Marketing and Advertising," requirements, and proposals for the format and content for the QR code's "Linked Information." Among other points, it recommends that the physical label shall be at least 1 inch by 2 inches and include the QR code and the Cyber Trust Mark, and have a minimum font size of 4 point font. It also specifies that the online cyber

nutrition label should be presented in both English and Spanish. The *Label Standard Cover Letter* also explains that the *Label Standard* leverages CTA-2120, *Design Requirements for a Label for IoT Device Cybersecurity* (CTA-2120), finding "that CTA 2120 provides for a straightforward, clear, flexible (i.e., vertical or horizontal layout) label design, including the necessary considerations to ensure a resolvable QR code (i.e., proper white space and sizing)." A user must follow a process similar to purchasing a product to view this standard, but we note it is available at zero cost. We propose to adopt the Lead Administrator's recommendations, with modifications as discussed below, and seek comment on this proposal. In addition to the proposed label requirements, CLAs and manufacturers must also agree to abide by a Trademark Use Agreement and accompanying branding guidance. The *IoT Labeling Order* and this Public Notice interchangeably refer to entities authorized to use the FCC IoT Label as manufacturers and grantees and, at times, as applicants. The *Label Standard* and *Renewal and Surveillance Document* refer to manufacturers as "grantees."

General Requirements for Label Display

The *Label Standard* recommends USCTM-certified products include the label on their packaging, either printed directly on the packaging or applied as an adhesive sticker. The *Label Standard* also recommends "[t]o build consumer trust in the Label and the registry content, the URL access via the QR code should be government hosted." We seek comment on these recommendations and generally on any actions we should consider regarding how the label is displayed. What steps should we take to protect the integrity of and consumer confidence in the FCC IoT Label and to discourage counterfeit usage and unauthorized reproduction beyond trademark infringement enforcement (e.g., watermarking)?

On-Package Label Design (2.1.1) (We include these numbers to help readers find the corresponding sections in the *Label Standard* and *Renewal and Surveillance Document*). The *Label Standard* provides recommendations regarding the design of the on-package ("physical")

label. It proposes that we base the label design requirements on CTA-2120 and incorporate CTA-2120 by reference into the USCTM Program requirements. The *Label Standard Cover Letter* notes that the Office of Management and Budget (OMB) encourages the federal government to adopt private sector-developed consensus standards, where those standards meet the government's purposes. Thus, we propose to adopt the *Label Standard* recommendations that the physical label design contain the QR code and "Bounding Box" as specified in CTA-2120. We also propose to adopt the *Label Standard* recommendation that the label's minimum font size should be 4 point font to provide flexibility to manufacturers displaying the physical label on their products. However, we note that CTA-2120's description of the physical label references a minimum font size of 5 point for legibility. We seek comment on this proposal and, specifically, whether the minimum font size for the label should be 4 point or 5 point font. Further, CTA-2120 specifies two potential orientations of the physical label: a "Horizontal Layout" and a "Vertical Layout," and includes technical QR Code specifications, which rely on international standards for QR codes and related printed symbols. We believe it promotes flexibility for both orientations to be permissible and propose to adopt this recommendation accordingly. To see a visual of these proposed orientations, we recommend commenters review CTA-2120.

The *Label Standard* recommends that, if an adhesive label is used, a URL, in addition to the QR code, should be printed on the label. We note that this recommendation is based on the assumption that the domain will be a ".gov" and thus, including the URL on the adhesive label furthers the goal of building consumer trust in the label and the registry content. CTA-2120 also specifies a "URL Zone" on the label with related content, scaling, and constraint parameters, which the *Label Standard* also recommends we adopt. CTA-2120 provides a graphic of its proposed "URL Zone," which we encourage commenters to review. While the *IoT Labeling NPRM* sought comment on whether to include both a non-Internet connected QR code and an Internet-connected URL on the label, the *IoT Labeling Order* ultimately concluded that a QR

code-embedded URL (one that links to a dynamic database of information) provides a simple way for consumers to access additional and current security information about the IoT product than what the label itself signifies. We seek comment on whether allowing for a printed URL in certain circumstances would conflict with the Commission's conclusion in the *IoT Labeling Order*. If not, under what circumstances should manufacturers also include a printed URL on the label (in addition to the QR code). For example, if adopted, should this requirement apply only to adhesive labels? If so, why? Should any such requirement apply to smaller IoT products that may be unable to accommodate a 1-inch by 2-inch label or in situations where there is no flat surface to support the scanning of a QR code? Should the inclusion of a URL be at the discretion of the entity authorized to use the FCC IoT Label? Is there a risk of consumer confusion if certain packages include a URL while others do not?

We also seek comment generally on whether CTA-2120 sufficiently addresses the FCC IoT Label requirements (e.g., QR code design and label design (e.g., size, white spaces), label placement (e.g., products where consumers may not see product packaging and products that do not have sufficient flat space to support a readable QR code)) and why. We note that some "stakeholders expressed concern about adopting a private sector developed consensus standard, noting that paid membership is required for participating on the CTA technical committee, and that that may be infeasible for some stakeholders." We seek comment on these concerns. We also do not propose to incorporate CTA-2120 by reference in its entirety at this time.

On-Package Label Dimensions (2.1.2). The *Label Standard* recommends the FCC IoT Label be at least 1-inch by 2-inches, noting that "[l]abel size is a critical consideration" and emphasizing that the label must be practical, flexible, recognizable, and legible. To allow additional flexibility for manufacturers to choose the label design and configuration that best fits their packaging and distributor needs, the *Label Standard* recommends three alternative options for smaller products that may be unable to accommodate a 1-inch by 2-inch label, which they

believe will not impact consumer recognition of the label or decrease its utility in educating consumers about the program and the IoT product:

- 1-inch by 1-inch label with the U.S. Cyber Trust Mark stylized shield logo and without the "U.S. Cyber Trust Mark" text; or
- ⅝-inch by ⅝-inch label with U.S. Cyber Trust Mark stylized shield logo included within a QR Code frame; or
- Where a product package has no single flat surface to accommodate the above options, the on-package label may consist of only the U.S. Cyber Trust Mark stylized shield logo and URL.

We seek comment on these recommendations and the proposed space-saving alternatives, particularly concerning options that do not include a QR code. We note that the *IoT Labeling Order* conditioned approval to use the Cyber Trust Mark on the label also bearing the QR Code. The *IoT Labeling Order* also specified that the QR code should be "scannable," and we acknowledge the potential for a QR code to be too small to be technically scannable. The *IoT Labeling Order* also noted that "some types of products might be customarily displayed in ways that make a one-size-fits-all approach inappropriate" and agreed that "we must consider how the label may be placed in ways that will be helpful to a consumer." While the *IoT Labeling Order* was focused on larger-sized appliances in this context, we recognize that this flexibility may be equally appropriate for smaller-sized IoT products. However, given the *IoT Labeling Order* requires that products bearing the FCC IoT Label, which includes the Cyber Trust Mark, must also include the corresponding QR Code, we seek comment on whether the space-saving alternatives that propose to omit the QR code conflict with the Commission's rules. Should small products instead be required to display the full FCC IoT Label (including both the Cyber Trust Mark and the QR code) elsewhere alongside the product, either via display collateral, if sold in stores or online, as discussed below? Would doing so lead to consumer confusion or erosion of consumer trust? We encourage commenters to offer proposed visual examples of

label design and configuration(s), which may include alternatives to the proposals recommended above.

Online or Catalog Display of Label (2.1.3). The *Label Standard* recommends that the webpage displaying a USCTM-certified product sold directly to the consumer via an online retail platform or through a catalog (whether via the manufacturer or third party retailers), may include the Cyber Trust Mark or the text "U.S. Cyber Trust Mark Certified" with linked navigation to the product's cyber nutrition label. The recommendation also proposes that the cyber nutrition label should be accessed via a hypertext link, a clickable QR code, or a hyperlinked Cyber Trust Mark. As above, we seek comment on whether the proposed alternatives that do not include the full FCC IoT Label (Cyber Trust Mark and QR code) conflict with the Commission's rules.

(Alternatives to) On Product Display of Label (2.1.4). The *Label Standard* recommends that the FCC IoT Label can be attached separately via display collateral (such as a hangtag or placard) to an IoT product, either in addition to the label's inclusion on product packaging, or in lieu of product packaging where products are displayed for sale without it. We propose to include this option in the program's branding guidance and seek comment on this recommendation.

Label Included in Product Documentation (2.1.5). We seek comment on the *Label Standard* recommendation that the FCC IoT Label should be included within the product's online *or* physical documentation (e.g., user guide), in anticipation of packaging disposal and the need for consumer access to the cyber nutrition label across the product's lifespan. We believe that this requirement should apply to both online *and* physical documentation in the event the physical documentation is lost or the information is updated. We propose to adopt this requirement, as modified, and seek comment.

Marketing and Advertising

The Label Standard recommends that where an IoT product has met the program's labeling requirements, the manufacturer should be permitted to also use the Cyber Trust Mark (with or

without the QR code) in the marketing and advertising of the USCTM-certified product (e.g., point of sale display, booth displays at trade shows, or a box front/back) in line with the label requirements and other branding guidelines developed by the Bureau. We agree that displaying the Cyber Trust Mark in marketing and advertising would contribute to consumer recognition and public education about the program. However, as above, we seek comment on whether allowing display of the Cyber Trust Mark without the QR code might lead to confusion about the baseline cybersecurity of the USCTM-certified product. If so, should we require that manufacturers engaging in marketing or advertising include the scannable QR code? We note that because manufacturers are precluded from construing, claiming, or implying that the U.S. Cyber Trust Mark constitutes an FCC or U.S. government endorsement of the product displaying the label or QR code, the Trademark Use Agreement and branding guidance will also note those limitations.

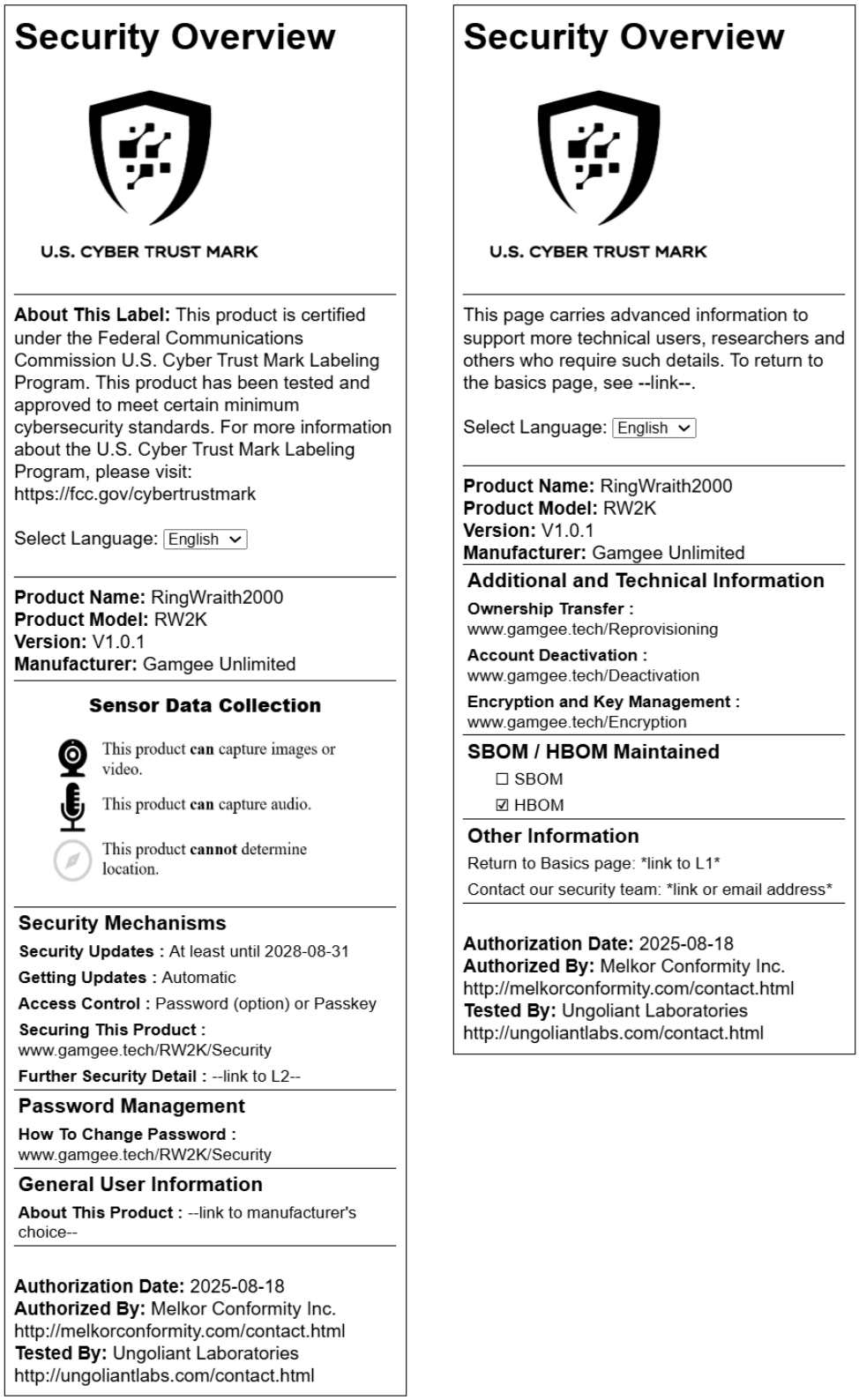
Linked Information

The *Label Standard* further leverages CTA-2120 in outlining a multi-layered label. The Stakeholder Committee found that "in CTA 2120, the QR-code linked information required for the registry is presented in a 'nutrition label'-like format, which will be familiar to many consumers . . . and the format is also friendly for display on mobile devices." It explains that the label is comprised of the on-package design ("Layer 0" or physical label) that links to the registry information presented to the consumer as the online cyber nutrition label. The nutrition label, in turn, consists of two layers in CTA-2120: "Layer 1" for consumer focused security information, and "Layer 2" for more technical users and researchers. "Linked Information" is defined as "[t]he standardized information fields presented on pages for the Layers L1 and L2 of the Label. The *IoT Labeling Order* required that the QR code-linked product information for consumers include eleven "essential" security-related data elements and provided that the information be displayed to the consumer in a simple, uniform way. CTA-2120 defines how data fields are to be presented in Layers 1 and 2, along with a standardized Application

Programming Interface (API) communication format. We seek comment on CTA-2120's proposed cyber nutrition label format as presented in Figure 2 of the *Label Standard*, and included below. We point out that Layer 1 of the CTA-2120 cyber nutrition label includes all of the elements required by the *IoT Labeling Order* except the requirement that the manufacturer disclose whether it maintains a Hardware Bill of Materials (HBOM) and/or a Software Bill of Materials (SBOM), which CTA-2120 presents on Layer 2. While many consumers may not understand the purpose of an HBOM/SBOM, we believe the *IoT Labeling Order* intended for all of the required data elements to appear on page one, or Layer 1 of the cyber nutrition label to "reduce potential burdens and focus on essential information." As such, we propose to decline to remove this data element (whether the manufacturer maintains an HBOM/SBOM) from Layer 1. Further, the *IoT Labeling Order*, while noting that "uniform registry elements will provide greater consistency for consumers and adoption of uniform registry elements is supported in the record" also acknowledged "the value in allowing manufacturers to include a second . . . 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." We seek comment on whether the *IoT Labeling Order* intended to allow for a Layer 2 and on the additional proposed revisions detailed below.

The *Label Standard* provides the following graphic of the cyber nutrition label that includes

Figure 1: Cyber Nutrition Label with Layer 1 and Layer 2



Layer 1 and Layer 2 as the consumer would view the information:

First, we note that the "About This Label" content states that "[t]his product has been tested and approved to meet certain minimum cybersecurity standards." We seek comment on whether this statement should instead use the term "*baseline* cybersecurity standards" as that term is consistently used throughout the *IoT Labeling Order* and aligns with NISTIR 8425. NIST notes the core baseline is "a starting point for manufacturers to use in identifying the cybersecurity capabilities their customers may expect from the IoT devices they create." In this same section, Figure 2 provides a drop-down menu for the selected language. In this regard, the *IoT Labeling Order* tasked the Lead Administrator with submitting recommendations as to whether the registry information should be available in additional languages, and if so, to recommend specific languages for inclusion. The *Label Standard* notes that the Stakeholder Committee recommended that the relevant information should be presented in both English and Spanish to encourage use and adoption of the program. Where the cyber nutrition label links to external websites maintained by the manufacturer, the *Label Standard* recommends that the manufacturer must provide the translated text on those sites. Further, the recommendation indicates that providing the information in both languages "should not pose a burden on manufacturers/label grantees because the HTML template for the linked information need only be translated into multiple languages once by the U.S. Cyber Trust Mark Program to ensure a consistent list of valid responses for each field, as specified in CTA 2120." We seek comment on these recommendations and on how best to ensure multilingual adaptability for the registry information and nutrition label.

Next, in response to the *IoT Labeling Order's* guidance that stakeholders consider the inclusion of certain security and privacy information on the cyber nutrition label (e.g., sensor data collection), Figure 2 includes a "Sensor Data Collection" section. The majority of the Stakeholder Committee members concluded that three sensors—camera/video capability, audio capability, and location determination—would be of greatest interest to consumers and recommended that they be disclosed by the manufacturer, as provided on Layer 1. We agree that

camera/video capability, audio capability, and location determination sensors should be disclosed and propose to adopt these disclosures, as recommended. We seek comment on this proposal and related symbols. Should these symbols comprise a standardized iconography set (consistent graphical icons) to indicate key features? If so, what standardized iconography set should be adopted? We also note that the icon for each of the three sensors are either bolded (if collected) or not bolded (if not collected) with a statement as to whether the IoT product "can" or "cannot" capture images/video/audio or determine location. We think these details are sufficiently descriptive to clearly identify to consumers the type of data the IoT product does or does not collect and seek comment on that determination.

Figure 2 next lists "Security Mechanisms" which includes the requirement that the cyber nutrition label include information about the product support end date under the heading "Security Updates" with the end date listed as: "At least until [Year-Month-Day]." We propose to modify the heading "Security Updates" to "Support Period" to clarify that the information includes (1) "the support period and end date for the support period," as required by the *IoT Labeling Order*, and (2) updates beyond security updates. We seek comment on this proposal. We also do not propose to allow for links to external websites maintained by the manufacturer except where it is necessary to provide additional information on how to configure the device securely in this section ("Securing This Product") of the cyber nutrition label. The Commission's rules require all essential registry data elements to be displayed in a "simple, uniform way," and we believe allowing additional external links beyond this unique case where additional information may be required would conflict with the program's intent. We seek comment on this determination.

Additionally, when a certification has lapsed due to the failure to renew, program compliance issues, withdrawal, or inclusion of the IoT product on the FCC Covered List, the *Label Standard* recommends that the cyber nutrition label be replaced with the following notice: "This product does not have a valid certification. If you would like to view information from when it was

certified, please click here." We agree that it is important for consumers to know if an IoT product bearing the FCC IoT Label is no longer authorized to do so. To minimize consumer confusion and burdens on manufacturers, we propose that the notice should read: "This product does not have a valid U.S. Cyber Trust Mark certification" and include the reason (e.g., failure to renew, withdrawal, inclusion on the FCC Covered List etc.). We seek comment on this proposal modification or an alternative statement for this purpose.

We also note that "Security Mechanisms" in Figure 2 includes the heading "Getting Updates" to comply with the *IoT Labeling Order* requirements, to include "[i]nformation as to whether software updates and patches are automatic and how to access security updates/patches if they are not automatic." We believe "Getting Updates" is accurate, but we seek comment on any changes to the wording to more clearly reflect the details of this requirement. Similarly, we believe the headings "Password Management," and "How To Change Password," accurately reflect the *IoT Labeling Order* requirement to include "[i]nstructions on how to change the default password [and] specifically state if the default password cannot be changed," but seek comment on whether the heading should be modified to more accurately describe instances where the password cannot be changed.

We ask commenters to provide feedback on whether any additional disclosures should be required for the cyber nutrition label, including whether physiological data will be collected, such as personally identifiable information, biometric, facial recognition, voice, fingerprints, or other behavioral data, and what icons or symbols should be required for those additional sensors, if any. We note that according to UL, a minority of the Stakeholder Committee members advocated for including radio frequency sensors and sensors that can collect physiological data, and recommended that, if physiological sensor information is required, then the relevant symbol provided in the Carnegie Mellon University Specification for CMU IoT Security and Privacy Label should be considered. Should these additional icons or symbols also be included in a standardized iconography set? If so, what standardized iconography set should be adopted? We

ask commenters to address other changes that should be made to the cyber nutrition label format to promote consumer understanding and ease of use, including the appropriate visual hierarchy of essential elements on the cyber nutrition label.

FCC Trademark Use Agreement and Branding Guidance

Conditionally approved CLAs will only be approved to accept and process applications and authorize use of the FCC IoT Label after the CLA has satisfied certain conditions, including executing a Trademark Use Agreement with the Commission, among others. The Trademark Use Agreement outlines the rights and expectations of CLAs related to granting authorization to use the USCTM, including sub-licensing to authorized manufacturers or other agents, such as advertising agencies, sales agents, and retailers. CLAs and sub-licensees will also be required to abide by certain Cyber Trust Mark branding guidance that governs the format of the FCC IoT Label and nutrition label, among other requirements. To inform the branding guidance, we seek comment on accessibility best practices for the nutrition label, including font readability, contrast ratios, and screen-reader compatibility for digital formats to ensure users with visual or other disabilities can access the nutrition label content. We also ask commenters to address alternative display formats for when the nutrition label is displayed on space-constrained or accessibility devices (i.e., smart watches, smart glasses, earbuds with text-to-speech, devices with small screens) such as digital labels or text-to-speech available via setup apps or companion software. We also seek comment on permitting alternative orientations or color schemes of the physical label to fit with existing product branding or design constraints, as well as co-branding or co-display with other certification marks (e.g., ETL Listed Mark, ISO Certified Mark) to reduce space usage and consumer confusion. We seek comment because we believe that these aspects of the brand guidance would benefit from public input and note that the Bureau may update that guidance from time to time without seeking comment unless doing so is required under the Administrative Procedure Act. Similarly, the Trademark Use Agreement itself is a living agreement that may be periodically and unilaterally amended by the FCC (with written notice to

the signing parties). We find that this approach gives the USCTM Program flexibility to adapt to changing market needs.

CERTIFICATION RENEWAL AND POST-MARKET SURVEILLANCE REQUIREMENTS

The Lead Administrator's *Renewal and Surveillance Document* offers recommendations to enable effective program oversight and accountability and to ensure grantees continually comply with all program requirements and updates thereto. It defines relevant key terms and recommends requirements for four processes: Certification Renewal, Post-Market Surveillance, Ad-Hoc Surveillance, and Complaint Handling. Among other points, it recommends how often grantees should be required to renew their authorization to bear the Mark and the processes required to do so (including a "Qualified Professional" role), post-market surveillance activities CLAs must conduct and grantees must participate in, follow-up actions following instances of non-compliance, random audits after certain precipitating events, and processes to receive and respond to complaints. We seek comment on these recommendations in general, and with proposed changes detailed below, including related definitions.

Initial Application and Certification Renewal

Initial and Renewal Applications. The *IoT Labeling Order* delegated authority to the Bureau to develop the application that manufacturers will use to request initial authority from a CLA to use the FCC IoT Label. We expect that the information manufacturers will include in their initial application for authority to use the FCC IoT Label will be similar to the information in their renewal application. As such, we first propose that, in addition to the information currently required by § 8.208, each initial application to use the FCC IoT Label shall include, at a minimum: the applicant's name, address, telephone number(s), email address(es), and website(s); contact information for personnel responsible for the application; the name and address of the agent located in the United States designated by the applicant to receive service of

process in the U.S.; the product name and type; the signed technical test report provided by an accredited and recognized CyberLAB. We anticipate each CLA will have its own electronic application submission processes and that adopting a required application format could interfere with CLA's established electronic processes. As such, we believe that describing the data elements that are required to be submitted to support the application satisfies this delegation of authority and we seek comment on this belief.

Although the *Renewal and Surveillance Document* does not describe what information applicants must provide to the CLA to initiate a renewal certification process, we propose that applicants filing for renewal certification should additionally provide the following: the date(s) on which each grantee received each authorization to use the Cyber Trust Mark; the authorizing CLA (if different); a description of changes to the IoT product since it was last evaluated; and a copy of all document(s) related to the granting of authorization to the grantee to use the Cyber Trust Mark, including the original application and all CyberLAB report(s). Below, we propose to require manufacturers to submit a test report conducted by a CyberLAB, as part of its renewal, that demonstrates that the product was tested against any new or revised USCTM Program requirements and 70% of the remaining requirements as part of their renewal application. We seek comment on whether this information provides CLAs sufficient data to manage and evaluate applications for initial and renewal applications for authorization to use the Cyber Trust Mark. If not, what additional information should be provided? As an alternative to certification renewal, would a term agreement on how long the Cyber Trust Mark may be used (subject to Commission renewal) in the Trademark Use Agreement and mechanisms for compliance with existing rules suffice? What are the related costs and benefits versus requiring a renewal?

Renewal Period. As recommended, the certification renewal process would confirm that the product continues to comply with the requirements applicable at the time of the initial authorization, as well as any new or revised requirements adopted since the initial certification or previously conducted renewal. The *Renewal and Surveillance Document* recommends that

grantees renew their certification every five years with an approved CLA. The *Renewal and Surveillance Cover Letter* explains that the Stakeholder Committee's preference for a five-year renewal period reflected concerns that a lesser period (e.g., three years) "would be overly burdensome on manufacturers and negatively impact program participation." Nevertheless, the *Renewal and Surveillance Cover Letter* separately recommends the Bureau consider whether a three-year renewal cycle is "*more* appropriate for a new program that is targeting evolving cybersecurity risks and seeking to build consumer trust," noting that three years is the typical timeframe for many cybersecurity certification programs currently in use globally.

We are concerned that a five-year renewal period does not adequately align with the fast-paced nature of IoT threat evolution, potentially leaving consumers with outdated cybersecurity protections. As such, we propose to adopt a three-year renewal cycle, which we believe strikes a balance between the Stakeholder Committee's recommended five-year renewal cycle and the annual renewal cycle the Commission initially proposed. We believe that ensuring consumers receive up-to-date information about the cybersecurity of the IoT product is more critical than the added, yet manageable, burden of more frequent manufacturer certification renewals. We seek comment on this belief. Are there other modifications to the recommended certification renewal process, including streamlined processes that might reduce burdens on manufacturers (e.g., automated reporting/patching, reduced scope/targeted review for stable products, leveraging existing certifications etc.)? We note that the *IoT Labeling Order* recognized "that certain IoT products, depending on their lifespan and risk level, may need different standards for renewal to achieve the FCC IoT Label," and tasked the Lead Administrator with considering such distinctions in recommending appropriate renewal timeframes. We seek comment on whether there are certain products or product classes for which a different renewal timeframe is appropriate. If so, what products and/or product classes and what timeframes would be appropriate? We also seek comment on the cost implications (in terms of renewal fees) of particular renewal timeframes.

Certification Renewal Process (2.1.1). The *Renewal and Surveillance Document* recommends six steps that a CLA must follow to conduct a product's certification renewal. In brief, the recommendations would require the CLA to: (1) perform an evaluation of the product against all new and/or revised program requirements since the product's certification or previous renewal; (2) perform a reevaluation of at least 50% of all applicable program requirements, excluding Security Documentation requirements; (3) verify certification for each Backend component for the product is current/valid; (4) conduct an in-person or remote audit to confirm grantee maintains required security documents and review implementation proofs performed within the last three months and information regarding the latest security/path updates; (5) confirm grantee maintains a USCTM Qualified Professional for the earlier of either the certification period or date of last renewal; and (6) withdraw the certification from the product registry with the required notice for products for which the certification renewal is due, but the grantee does not seek renewal. We propose to adopt the first five steps as recommended, with proposed changes to step two, and seek comment. We do not propose to adopt step six at this time, as details related to the program registry are still pending, but seek comment below on steps to take to withdraw a certification from the registry.

First, we agree with and propose to adopt the recommendation that the renewal should include an evaluation of the IoT product against any new or revised program requirements adopted since the product's certification or previous renewal. However, we are concerned that the recommended minimum "50% sampling of all applicable [USCTM Program technical] requirements" for each product, excluding Security Documentation, is unclear and may not detect a sufficient number of products with only one instance of non-compliance. Since the recommendation requires the CLA to first perform an evaluation of the product against all new and/or revised requirements in the first instance, we propose to require reevaluation of at least 70% of all *remaining* requirements (those that are not new and/or revised since the product's last evaluation), as the next step, followed by reevaluation of 100% of these remaining requirements if at least one

instance of non-compliance is found. We also propose to require manufacturers to submit a test report conducted by a CyberLAB, as part of its renewal, testing the product against any new or revised USCTM Program requirements and 70% of the remaining requirements (those that are not new or revised) as part of their renewal application. We believe that doing so will result in more effectively identifying instances of non-compliance and we seek comment on this determination. We note that while requiring an even higher sampling percentage (greater than 70%) would offer more protection in detecting instances of non-compliance, the difference may not be significant enough to warrant the increased burden on participants. Moreover, we anticipate adjusting the renewal testing strategy as informed by the certification testing experience over multiple years. We also seek comment on who would identify the 70% of all remaining requirements that should be evaluated (e.g., the CLA). If renewal applicants could identify the 70% of requirements to be evaluated themselves, we are concerned that would create an incentive to only evaluate the requirements that are least costly to retest. In the alternative, or in addition, should we establish a subset of testing that would identify critical security requirements that should always be evaluated for renewal? If so, what should those critical security requirements be? Would testing the same 70% of requirements for renewal each time risk creating a blind spot where renewal applicants do not consistently maintain compliance with our rules? We seek comment on these renewal proposals and any other alternatives that may be more effective. Will it be necessary for us to define how an individual, discrete requirement is measured, for the purposes of this sampling percentage, when the technical requirements are adopted? If so, what should be considered "one" requirement? Would a complete recertification process, in lieu of maintaining a distinct renewal procedure, offer a more straightforward and less burdensome approach for grantees and CLAs?

U.S. Cyber Trust Mark Qualified Professional (2.1.2). The *Renewal and Surveillance Document* recommends that the grantee appoint and maintain a USCTM "Qualified Professional" to reinforce ongoing conformity with the USCTM Program's requirements and provide consistent

identification of compliance-relevant changes to certified IoT products. Grantees must notify the CLA that conducted the original application assessment of any changes to the product or relevant documentation that may impact compliance to the USCTM Program, as identified by the Qualified Professional. The *Renewal and Surveillance Cover Letter* indicates that precedent exists for this requirement, stating that "relying on knowledgeable and specially qualified staff to identify changes that could impact compliance is used in other certification programs." We agree that having dedicated personnel to monitor product changes and changes to program requirements would contribute to ongoing conformity and propose to adopt the Qualified Professional requirement as recommended and seek comment as outlined below.

The *Renewal and Surveillance Document* recommends that to be designated as a USCTM Qualified Professional, a staff member (including a contractor, vendor, or similar agent) must obtain certain qualifications, including completing an "approved course" and passing an exam on the USCTM Program requirements and confirming receipt of major changes to the USCTM Program from the Lead Administrator and the FCC. The *Renewal and Surveillance Cover Letter* further notes that USCTM Qualified Professional training and assessments (the "approved course") could be developed by the Lead Administrator and/or the CLAs. To maintain status as a Qualified Professional, the *Renewal and Surveillance Document* recommends the staff member must confirm receipt of major changes to the USCTM Program from the Lead Administrator and the FCC, that impact its role and activities, and repeat the approved course and exam requirements every three years. If the designated USCTM Qualified Professional leaves the grantee's organization or is no longer serving in the role, the *Renewal and Surveillance Document* recommends that the grantee must notify the relevant CLA(s) and fill the vacancy within six months.

We seek comment on these recommendations generally, including whether the Lead Administrator or CLA should be responsible for administering the approved course or whether the training may be conducted in-house to each grantee. What aspects of the program's

requirements should be included in the approved training and assessment course? Should the content of the approved course change every three years? Is three years the appropriate cadence for regular exams? How should "major" changes be defined for purposes of the Qualified Professional role? How often should the Qualified Professional confirm receipt of information regarding major changes to the USCTM Program once designated? Should these major changes be relayed to the grantee and Qualified Professional from the Lead Administrator or the CLA? Would CLAs be required to communicate these changes to grantees already (e.g., through their ISO/IEC 17065 accreditation requirements)? Are there other qualifications that the Qualified Professional should meet? We presume that if a USCTM Qualified Professional were to move from one grantee organization to another, they may carry their status over to another organization since the same approved training and exam will be used across grantees. We seek comment on this presumption. We propose to adopt the *Renewal and Surveillance Document*'s recommendation that if a Qualified Professional leaves an organization, the grantee must notify the CLA that granted the product's certification of the vacancy. We seek comment on the timeframe within which the position must be filed. Are there other ways for grantees to ensure CLAs are kept informed regarding any relevant product changes that may impact compliance with the USCTM Program? Do the expected benefits of such a role outweigh the costs of maintaining a certification program, and applying for, obtaining, and maintaining the certification, or should we decline to adopt this recommendation? We seek comment on these questions and on any gaps or alternatives to the Qualified Professional recommendation.

Certification Renewal Timing (2.1.3). The *Renewal and Surveillance Document* recommends that certification renewals be due at least six months prior to expiration. It recommends allowing grantees a "grace period" to continue using the Mark for an additional six months after the original expiration date while their renewal request is under review by a CLA. We seek comment on this recommendation, which essentially provides for a combined one-year renewal application period before a grantee's certification lapses: a six-month period for the grantee to

apply and an additional six month period for the CLA to evaluate the renewal application. We are concerned that this one-year period extends the timeframe for completing renewal evaluations beyond what may be necessary to provide flexibility to grantees and CLAs. Indeed, allowing a cumulative one-year renewal period risks diminishing the integrity of the certification process as a whole. As such, to ensure continued compliance and allow grantees to renew an existing certification rather than reapply for certification, we propose to require that grantees apply for renewal at least 90 calendar days before the product's certification expiration date and we require CLAs to complete their renewal evaluation within 90 calendar days of receiving the grantee's application. We think this timeframe can ensure timely review and renewal of active USCTM certifications and seek comment on this proposal. In cases where CLAs fail to complete their evaluation within 90 calendar days, what process should grantees follow to protect the integrity of the USCTM Program? What impact, if any, should this have on the product's certification expiration date? As noted above, we propose that the manufacturer would apply for certification renewal via an application with required information.

In addition to the grantee being responsible for filing for renewal, we believe it is the responsibility of each CLA to track the renewal due dates of the products they certify; notify the grantee of renewal deadlines; and subsequently, notify the Lead Administrator and the Bureau of any failure of the grantee to timely file for renewal. We seek comment on these requirements, including comments on a structured, uniform process for how and when each CLA should notify grantees and, separately, the Lead Administrator and the Bureau. If the grantee chooses to renew with a new CLA, the grantee is required to notify the original CLA. We propose that while the CLA is required to remind grantees of upcoming renewal deadlines, the failure of the CLA to do so does not excuse the grantee from filing a timely renewal application and seek comment on this proposal. We further propose that these CLA responsibilities will follow the CLA who assumes the responsibilities of a withdrawn or terminated CLA. We propose that the product's certification should automatically terminate on the expiration date if the grantee fails to timely

apply for renewal. We seek comment on this proposal. What additional steps should be taken, and by whom, to ensure that the product certification is withdrawn from the registry as a result of an untimely renewal? We want to encourage timely renewal to protect the integrity of the USCTM Program and ensure consumers have current information about their IoT products and seek comment generally on processes and timing to ensure such integrity.

Post-Market Surveillance Requirements (2.2). The *Renewal and Surveillance Document* recommends requiring all CLAs to perform post-market surveillance activities in accordance with ISO/IEC 17065 and the additional requirements outlined in the *Renewal and Surveillance Document*. The *Renewal and Surveillance Document* provides a multi-step process that CLAs would be required to follow to fulfill their post-market surveillance obligations. The process includes the following: Sample Test Plan; Sample Selection; Sample Rate, Selection Timeframe, and Report; Obtain Sample; Evaluation; and Follow-up Actions. We seek comment on this recommended process generally and as detailed below.

Sample Test Plan. The *Renewal and Surveillance Document* recommends CLAs have a written Sample Test (surveillance) Plan describing how they will ensure that the proper percentage of representative certificated products are tested. The *Renewal and Surveillance Document* provides a list of information that CLAs would be required to provide in writing to the grantee. In brief, it recommends that the CLA must notify the grantee in writing that: (1) CLAs must conduct post-market surveillance sampling; (2) the grantee must ensure the availability of production samples at least until the longer of either the end of the support period communicated on the product registry or no less than one year after the last production dates, whichever period is longer; (3) the grantee may be required to submit the product for post-market surveillance testing and that these samples may be requested at any time by the FCC or the CLA; and (4) the failure to provide samples within 30 days of the request could result in certification withdrawal. We seek comment on these requirements.

In particular, given that there are no recommended minimum parameters provided for the Sample Test Plan, we propose to require CLAs to submit these plans to the Lead Administrator and to the Bureau, upon request, to review and approve to ensure greater consistency among CLAs. We think the Lead Administrator (subject to Bureau oversight) is in the best position to determine whether a CLA's surveillance plan is sufficiently robust to identify and mitigate evolving vulnerabilities throughout an IoT product's life cycle and seek comment on that determination. We also seek comment on what minimum elements should be required for the Lead Administrator to determine that a Sample Test Plan is sufficiently robust. We also note that the *Renewal and Surveillance Document* includes a recommendation that CLAs submit an annual sampling plan specific for a given 12-month period to the FCC in September. We do not believe this requirement is necessary, as drafted. Instead, we propose requiring CLAs to submit an annual Sample Test Plan to the Lead Administrator in September and provide their grantees a copy of the Lead Administrator approved Sample Test Plan. These plans should be provided by the Lead Administrator to the Bureau upon request. We note that the *Renewal and Surveillance Document* assumes that the CLA is required to provide grantees with a Sample Test Plan but does not provide a definitive requirement. We also propose to require the Lead Administrator, in its role as a CLA, to submit its Sample Test Plan to the Bureau for review and seek comment on these proposals. Should we further require that all Sample Test Plans be treated as presumptively confidential and require CLAs to maintain this confidentiality? Alternatively, should we refrain from requiring CLAs to provide grantees a copy of their Sample Test Plan to discourage attempts to escape sampling and surveillance?

Sample Selection. The *Renewal and Surveillance Document* recommends samples audited by a CLA be selected from "the products certified or renewed by that CLA over the current year or the 4-year period directly preceding submission of the sampling plan to the FCC," and that a product may only be selected once for surveillance within its certification renewal period unless requested by the FCC. When selecting the product samples to be audited, the *Renewal and*

Surveillance Document provides a list of seven criteria that CLAs shall use to prioritize selection, including: (a) broad grantee and laboratory representation; (b) representation of the full range of product types certified; (c) recent security events; (d) representation across previous years of certifications issues, (e) new grantee; (f) grantees with a history of non-compliance; and (g) requests from the FCC for an audit to be performed on specific product or a group of products. We seek comment on these recommended requirements and related priorities for sample selection.

Consistent with our proposals above, we seek comment on modifying the recommended requirement that samples be selected from "the products certified or renewed by that CLA over the current year or the 4-year period directly preceding submission of the sampling plan to the FCC" in two ways. First, as noted above, we are concerned that a five-year renewal period may leave consumers vulnerable to cyber threats resulting from outdated product security. Similarly, we believe that requiring a product to be audited only once every five years (within the certification period) may be insufficient to ensure ongoing compliance, given the rapid evolution of cybersecurity threats. As such, consistent with our proposal to require a three-year cycle for certification renewal, we propose to require a sample be selected from the products certified or renewed by a CLA over the current year or the two-year period directly preceding submission of the sampling plan and that a product should only be selected once for audit within its three-year certification period, unless otherwise requested by the Bureau. We seek comment on this determination. Second, we propose to modify the language "preceding submission of the sampling plan to the FCC" to "preceding submission of the sampling plan to the Lead Administrator" consistent with our proposal above to require CLAs to submit their Sample Test Plans to the Lead Administrator. We seek comment on these changes. Commenters should also address whether IoT products with "higher risks" to consumers if they are exploited (e.g., remote monitoring/home security cameras, baby monitors, products marketed to children) should be subject to more frequent surveillance. Do the seven proposed criteria effectively prioritize the

IoT products most likely to negatively impact consumers if their security flaws are exploited (e.g., smart home devices, children's products)? Are there additional criteria that should be mandated for audit selection?

Sample Rate, Selection Timeframe, and Report. The *Renewal and Surveillance Document* recommends that CLAs adhere to several sampling, selection, and report requirements. We propose to adopt these requirements, with changes discussed below, and seek comment. We propose to adopt the recommendation that the total number of products selected for surveillance by a CLA be at least three percent of the total number of products certified or renewed by the CLA during the prior calendar year. Nevertheless, we seek comment on whether this percentage strikes the right balance between minimizing the burden on grantees and CLAs, while maintaining consumer trust that non-compliant products are identified. If not, what percentage of the total products certified or renewed by the CLA during the prior calendar year would yield a more effective sample rate? Why? Further, we propose that, as described above, "products selected for surveillance by the CLA shall be selected from the devices certified or renewed by the CLA over the current calendar year *or previous 2 calendar years*" for consistency with our proposal for a three-year renewal certification cycle. We note that using a fixed calendar year baseline for surveillance (rather than a rolling window of time) provides CLAs with a fixed, unchanging target sample size and greater predictability, and it potentially prevents redundant oversight of recently approved devices. We seek comment on this determination. We also seek comment on the format and content of the annual post-market surveillance reports the *Renewal and Surveillance Document* recommends CLAs submit to the Commission on June 30. We propose that these annual CLA reports be submitted to the Lead Administrator rather than the FCC. We further propose to require the Lead Administrator to submit an annual report to the Bureau of the CLAs' post-market surveillance activities and findings and we now seek comment on the format and date upon which this report should be filed.

Obtain Sample. As described above, failure of the grantee to submit a product sample within 30 days of the request may result in withdrawal of the product's authorization to use the Mark. The *Renewal and Surveillance Document* recommends the CLA be required to "notify the FCC if a grantee refuses, or fails to comply with, a request for a sample." We believe the Lead Administrator is in the best position to receive these notifications and address them in the first instance, and thus we propose to require that the CLA should notify the Lead Administrator if a grantee refuses or fails to comply with a sample request. We further propose that the Lead Administrator must notify the Bureau if it is unable to resolve the failure to comply in a reasonable period of time. We seek comment on these proposals, including what constitutes a reasonable period of time for manufacturers to comply with a request for a sample, and the structure and format in which the Bureau should be notified of failures to comply.

The *Renewal and Surveillance Document* recommends, and we propose to adopt, that CLAs should obtain a product sample by requesting that the grantee either submit a product sample from their production stock or purchasing a product sample from the marketplace and deliver it to the CLA. The *Renewal and Surveillance Document* also recommends the applicant provide justification in its application if it would be overly burdensome to keep a production sample on hand or if the production run for the product is limited, which we propose to adopt. We also propose to adopt the recommendation that the CLA will determine whether the applicant's justification is acceptable and retain this determination within the application record. The *Renewal and Surveillance Document* further recommends that a grantee's statement that a product is no longer manufactured or will not be marketed in the United States should not serve as sufficient justification for failing to provide a product sample to a CLA or the FCC. We propose to adopt this recommendation, but replace "or the FCC" with "or to the Bureau upon request" for this requirement, as we do not expect the Commission will be handling product samples directly. We seek comment on these proposals and related details.

To ensure that grantees are not submitting the same unit used during initial certification testing, we propose to require that grantees submit a sample from their latest production line and seek comment on this proposal. Are there other risks associated with having the grantee submit its own product sample to the CLA for post-market surveillance? How should we ensure that grantees submit "representative" samples for surveillance testing? Alternatively, should we require CLAs to specify a random or otherwise objective method for selecting a sample from production stock? Or should we require independent marketplace acquisition in certain circumstances? If a CLA or the Bureau is made aware through consumer complaints or otherwise that a grantee's sample was not representative, should such a determination potentially be grounds for withdrawal of a product's certification? We seek comment on this proposal, including what constitutes a reasonable period of time for manufacturers to comply with a request for a representative sample, which may require a different or longer timeframe to obtain and compile than a standard physical product sample.

Evaluation. The *Renewal and Surveillance Document* recommends certain procedures and requirements by which the product sample shall be evaluated by the CLA to determine compliance with the USCTM Program requirements, including parameters for how a CLA should perform product testing and compare the test data, and where the CLA must perform the testing. The requirements include the obligation of the CLA to review implementation proofs, verify backend component certifications, examine the sample packaging for compliance, and final review and signature by appropriate personnel. We seek comment on each of the evaluation procedures and requirements. In particular, we seek comment on the recommendation that CLAs perform "sufficient testing to provide a high level of confidence" that the product sample complies with program requirements. Under this requirement, complete testing to all program requirements is not required; however, testing is required for those requirements most likely to be in non-compliance. We find this recommendation vague. While we understand that the CLAs are likely in the best position to determine the degree of testing necessary, we seek

comment on whether this can be quantified into a statistical standard (e.g., a low probability of certifying a product such that the percentage of non-compliant units is no more than X%)? If so, what statistical standard should be used? Alternatively, should sample selection for surveillance trigger a certification renewal? We seek comment on how this would impact costs to manufacturers, if so. We also seek comment on any additional ways to provide greater specificity while prioritizing efficient and targeted risk-based surveillance testing.

The *Renewal and Surveillance Document* also recommends requiring the CLA to perform post-market surveillance "testing at either a CLA-run lab or another CyberLAB but not at a manufacturer's in-house lab." We note that the *IoT Labeling Order* defined "in-house labs" as those in-house to the manufacturer. We find this recommendation consistent with the intent of the *IoT Labeling Order* and propose to adopt it with modifications. Specifically, we propose to clarify that the testing could be completed *through* a CLA-run lab or recognized CyberLAB, but not a manufacturer's in-house lab. We seek comment on this assessment. The *Renewal and Surveillance Document* also recommends that post-market surveillance testing should be performed by the same lab that performed the original evaluation whenever possible. We seek comment on this requirement, particularly whether there are any specific considerations the CLA should account for when selecting the product's post-market surveillance testing lab (e.g., the same lab that conducted the original testing, which may result in cost savings due to the lab's prior knowledge of the IoT product, or a different lab to provide an additional level of oversight). The *Renewal and Surveillance Document* further recommends that the CLA "shall confirm that the grantee has made no changes to the device, applications, or backend/cloud services that impact compliance" to the program requirements. We seek comment on whether there are certain permissive changes that may not impact the product's compliance, but should still be verified since they may pose a potential risk if improperly implemented (e.g., moving backend cloud services from one provider to another, adding new functional features that interact with the device).

Follow-up Actions. The *Renewal and Surveillance Document* recommends several actions CLAs must take based on the findings of the post-market surveillance evaluation. In particular, it provides the steps the CLA must take if a sample product fails to comply with program requirements, which includes notifying the grantee and providing the details of the non-compliance to the FCC by either submitting an inquiry to CyberTrustMark@fcc.gov or via another process designated by the Commission. We note that these recommendations differ from the *IoT Labeling Order's* general parameters for post-market surveillance reporting that CLAs should follow, which include: immediately providing written notice to the grantee, the Lead Administrator, and the Commission when the CLA determines that a product fails to comply with the technical regulations for that product; providing the grantee 20 days to cure the deficiency or lose authority to use the IoT Label; and providing periodic reports to the Lead Administrator and the Bureau, upon request, of their post-market surveillance activities and findings in the format and by the date specified by the Bureau. The *IoT Labeling Order* also required the stakeholder recommendations to include procedures to be followed if a grantee's approval to display the USCTM is terminated "based on 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."

Given the guidance provided in the *IoT Labeling Order*, and to the extent the recommended follow-up actions deviate from the Commission's direction, we seek comment on what additional follow up actions (e.g. notifications, reporting, resolution processes) or termination procedures should be followed as a result of a product's failure to comply with program requirements or disqualification from participating in the USCTM Program. In particular, we note that the Bureau previously sought comment on the recommended procedures to follow when a product loses its authority to use the FCC IoT Label (e.g., expiration or revocation). The record generally supported implementation of product control measures similar to the disqualification procedures adopted for the ENERGY STAR program. We seek comment on

whether similar disqualification procedures should be implemented for this program and whether there are additional actions the CLA must take beyond those already enumerated in our rules to effectuate the disqualification of the product (e.g., tracking and recording the manufacturer's implementation of product control measures).

We do propose that CLAs shall assist the Bureau in policing unauthorized use of the U.S. Cyber Trust Mark through post-market surveillance and auditing activities, and by notifying the Lead Administrator and FCC as soon as it becomes aware of any use by any other person of a name, trade name, trademark, domain name, email address, metatag, AdWords (or similar search term), mode of advertising, or anything that may reasonably constitute (i) infringement of, (ii) unfair competition with, or (iii) passing off as, any of the Cyber Trust Marks. In addition to promptly reporting the improper usage, the CLAs shall provide relevant material, if available, to the Lead Administrator.

Finally, we note that the *IoT Labeling Order* delegated authority to the Bureau, in connection with the Office of the Managing Director, to consider issues related to fees charged by CLAs and the Lead Administrator to cover the costs of performing their duties and to ensure that these fees do not become onerous and deter participation in the program. While we agree with the Commission that market competition will prevent fees from become overly burdensome, we seek comment on any additional steps, if any, we should take to ensure fees are reasonable, competitive, and accessible while covering the administrators' costs. For example, should the Commission require CLAs to publicize the fees they charge to manufacturers? Does the number of CLAs ensure sufficient competition to avoid onerous fees to manufacturers applying for authorization to use the Mark?

Ad-Hoc Surveillance

The *Renewal and Surveillance Document* recommends that, in addition to annual post-market surveillance, CLAs be required to perform ad-hoc surveillance evaluations, which they

recommend the FCC initiate, in response to large cyber events impacting consumer IoT products. As part of this recommendation, a committee consisting of representatives from each CLA must convene within 30 days of the FCC initiation to determine if the surveillance audit is justified, create a decision tree as an objective basis for its decision (scope, logistics, limitations, and risk model), and either provide a surveillance plan to the FCC if an audit is deemed necessary, or provide the FCC a justification, if it is not. Further, following Commission approval of the surveillance plan, the recommendation states that product sampling will be obtained and evaluation testing will be conducted consistent with post-market surveillance requirements, and that reporting outcomes must be communicated to the FCC as defined by the surveillance plan. It also proposes that the FCC communicate ad-hoc surveillance plans to approved accreditation bodies. We seek comment on these recommendations and related details.

We propose that the Bureau, rather than only the full Commission, may initiate an ad-hoc surveillance evaluation where there is a "large cyber event" and we seek comment on whether there are other events or circumstances that may necessitate such an evaluation. We also clarify that if we adopt this ad-hoc surveillance process, the Lead Administrator would be responsible for convening representatives of the CLAs to make the required submissions to the Bureau, and we seek comment on these clarifications. We also seek comment on requiring each CLA to make a representative available for this purpose as a condition of its final CLA approval. Further, should the Lead Administrator and/or a CLA committee be empowered to initiate certain ad-hoc surveillance activities on their own without Bureau initiation? If so, under what circumstances and processes? Additionally, we believe that the requirement that the CLA committee develop either a surveillance plan or a justification for no ad-hoc audit should include a firm timeframe for submission to the Bureau and seek comment on the appropriate timeframe. Given the potential security issues that may be involved with the investigation of a large cyber event, should these submissions be presumed confidential and be submitted via paper marked confidential through the FCC, Office of the Secretary? We also propose that the Bureau would

be the final arbiter of whether an ad-hoc surveillance evaluation is justified. Are there foreseeable circumstances when no ad-hoc audit will be justified following a large cyber incident? We believe that ad-hoc surveillance following large cyber incidents with known impacts to consumer IoT products will likely be justified and seek comment on this belief.

We propose the Lead Administrator separately, or in conjunction with the "reporting outcomes" from the surveillance plan, submit a post-audit report identifying and addressing (including remediation timelines) any gaps in surveillance evaluation processes or other systemic breakdowns in product security as a result of the cyber event. We seek comment on this requirement.

Handling of Complaints

The *IoT Labeling Order* determined the Commission and the CLAs will receive complaints regarding noncompliant displays of the Cyber Trust Mark and delegated authority to the Bureau, in coordination with the Consumer and Governmental Affairs Bureau, to determine the process for receiving and responding to complaints. The *IoT Labeling Order* also required CLAs to refer these complaints to the Lead Administrator who would then notify the Bureau. The Bureau previously sought comment on the processes for receiving and responding to complaints and received several comments addressing the issue.

The *Renewal and Surveillance Document* recommends that complaints be submitted against USCTM-certified products to any CLA through their standard complaints management process, includes the steps the CLA must take after receiving a complaint, and recommends a 30-day timeframe for the CLA to file a follow-up report on the actions taken. In brief, the recommendations require the CLA receiving the complaint to determine if the complaint is within the scope of the USCTM Program requirements, confirm the certification status of the product, notify the Bureau of any misuse or misrepresentation of the trademark, and transfer the complaint to the certifying CLA if the product is properly certified. Thereafter, the certifying

CLA must determine if the product is compliant or non-compliant, and if non-compliant, immediately notify the grantee and the FCC, and provide the FCC with follow up reports on the actions to be taken to correct the non-compliance. We seek comment on what additional procedures should be required in handling complaints. We propose that the CLA must notify the grantee and the Lead Administrator regarding the determined compliance or non-compliance (rather than the Commission). In turn, the Lead Administrator must notify the Bureau in the format and by a date specified by the Bureau. We seek comment on the format and structure of these notifications. Finally, we seek comment on whether a standing CLA committee comprised of a representative from each CLA responsible for addressing both complaints and ad-hoc surveillance is appropriate.

Procedures for Administrator Withdrawal or Termination

Lead Administrator Withdrawal. The *IoT Labeling Order* delegated authority to the Bureau to develop the procedures for withdrawal and termination of the Lead Administrator and CLAs. The Bureau previously sought comment on procedures for withdrawal and removal of the Lead Administrator. We propose that a Lead Administrator seeking to withdraw from their position as Lead Administrator of the program, while remaining a CLA, must provide written electronic notice to the Chief, Public Safety and Homeland Security Bureau through the appropriate FCC Docket of its intention to withdraw and include the effective date of the withdrawal. For entities seeking to withdraw as both the Lead Administrator and a CLA, we expect they would take the actions described in this section and the following section regarding CLA withdrawal. We seek comment on whether we should require specified advance notice period for the Lead Administrator to provide its intent to withdrawal. Several parties in the response to the *Delegated Authority Notice* recommend setting term limits for the Lead Administrator or some other form of ongoing reevaluation. We seek comment on these recommendations and what the criteria for reevaluation should include.

We propose that upon receipt of notice of the Lead Administrator's intention to withdraw from the USCTM Program, the Bureau will release a Public Notice opening a filing window for Lead Administrator applications, which is supported by the record. We also propose that the Lead Administrator be required to cooperate with the Bureau to transfer responsibilities to a new Lead Administrator, including the transfer of USCTM Program records, even if such transfer occurs after the effective date of the Lead Administrator's withdrawal. We propose that the records the Lead Administrator would be required to transfer to the new Lead Administrator include, but not be limited to, those associated with the Lead Administrator's recognition of CyberLABs to include approved, denied, and pending requests for CyberLAB recognition; complaints (pending and completed); audits; renewals; and Trademark Use Agreements. We recognize that Lead Administrators may develop data systems to support administration of the Program. As part of the transfer, we seek comment on whether supplementary documentation describing the structure and operation of such database systems should be made available to facilitate a smooth transition. We further seek comment on what format records should be shared. We seek comment on this requirement and any additional information that should be provided by the outgoing Lead Administrator to the new Lead Administrator. What additional actions should the Lead Administrator take for a smooth transition to a new Lead Administrator without interruption to the program?

CLA Withdrawal. We note that the *IoT Labeling Order* set forth several parameters regarding a CLA's voluntary or involuntary withdrawal from the USCTM Program. In addition to those requirements, we propose the CLA be required to provide 30 days advance notice to the Lead Administrator, the manufacturers the CLA has authorized to use the FCC IoT Label, and pending applicants of their intent to withdraw and the effective date of the withdrawal. If the CLA is simultaneously withdrawing as the Lead Administrator, we would expect such entity to provide the advance notice to the Chief, Public Safety and Homeland Security Bureau, and cooperate with the Bureau to transfer responsibilities and records, as outlined above. We seek comment on

requiring the notice to the manufacturer to include a reminder that they should choose a new CLA for oversight of its authorized product within 30 days of receipt of the CLA notice of withdrawal and remind the manufacturer that they should notify the Lead Administrator, the withdrawing CLA, and the new CLA, of the new CLA selection.

We also propose that CLAs be required to provide copies of all records relating to applications and authorization to use the FCC IoT Label, the use of the FCC IoT Label, post-market surveillance, and complaints with respect to rules of the USCTM Program to the Lead Administrator upon request by the Lead Administrator, including but not limited to, when they withdraw from the program and which may be requested before or after the effective date of the CLA's withdrawal. We propose to require each CLA to cooperate with the Lead Administrator with transferring responsibilities to the manufacturer's new CLA of choice, including the transfer of USCTM Program records even if such transfer occurs after the effective date of the CLA's withdrawal. We propose that the records the CLA would be required to transfer to the new CLA include (but would not be limited to) those associated with the CLA's processing of manufacturer applications to include approved, denied, and pending applications; complaints (pending and completed); audits; renewals; and Trademark Use Agreements. We propose to require CLAs to retain these records for a minimum of the term of the Trademark Use Agreement, plus five years thereafter. We also propose to require CLAs to provide the Bureau with a copy of the grantee's records no later than five business days after receiving a request to do so. Administrators will also be required to comply with the timeframes applicable for any federal records as to preservation and disposal of such records. What format should these records be provided in and should additional documentation relating to data systems and administration be shared? We seek comment on these requirements and any additional information or actions that a withdrawing CLA take for a smooth transition to a new CLA without interruption to the program? Finally, we seek comment on whether there are compensation issues that should be considered regarding these proposed requirements (e.g., CLA

sharing of fees relating to their proportion of renewal or auditing work completed, proportion of CLA cost sharing for Lead Administrator incurred expenses for performing duties on behalf of the program as a whole).

CLA Termination. The *IoT Labeling Order* provided delegated authority to the Bureau to determine if a CLA's authority should be terminated for failure to uphold the competencies or accreditations required under the USCTM Program and delegated authority to the Bureau to terminate the CLA's authority. The *IoT Labeling Order* also provides that the CLA's authority under the USCTM Program will automatically terminate if the CLA "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 [the IoT Labeling Order] as precluding authorization as a CLA." There may also be circumstances under which the arrangement with a CLA is voluntarily terminated, including but not limited to the CLA's withdrawal, provided there is sufficient notice to arrange a transition. We seek comment on whether there are other areas we should consider for terminating CLA authority, such as, for example, violations of the Trademark Use Agreement, violations of the Act, or if the entity is suspended or debarred from other Commission programs. Noting the importance of CLAs' continued compliance with USCTM Program requirements, we seek comment on imposing an ongoing obligation for CLAs to disclose to the Lead Administrator and the Bureau any law or rule that would preclude it from acting as an administrator of the program. The Commission also determined that due to the public safety importance of a CLA having the requisite qualifications and adhering to the USCTM Program rules, (1) the termination of authority should be expeditious; and (2) the Bureau should provide the CLA with notice of its intention to terminate the CLA's authority and provide the CLA a reasonable opportunity to respond; but (3) no more than 20 days should pass before reaching a decision on the termination. The Bureau may suspend the CLA's ability to issue labeling authorizations during the pendency of such consideration, if appropriate. We propose that if the deficiencies are not satisfactorily corrected within 20 days, two things will

happen. First, the Bureau will terminate the CLA's authorization via Public Notice. Second, the Lead Administrator will provide written notice to the CLA's authorized manufacturers about the CLA's termination and direct each manufacturer to select a new CLA. We seek comment on the timeline for manufacturers to make a new CLA election, which we believe should be timely to ensure there is a limited break in CLA oversight of IoT products certified under the USCTM Program. We seek comment on this process. We also seek comment on what, if any, deficiencies may be of sufficient concern to the USCTM Program that the Bureau should not provide 20 days for the CLA to cure. We seek comment on using the same CLA records transfer process here that we adopt when a CLA authority is terminated. We also ask commenters to address the most effective and streamlined way for a grantee to transfer to a new CLA in this context, particularly in those instances where transferring the grantee's data from a terminated CLA to a new CLA is not an option. In general, we believe that the Lead Administrator is in the best position to reassign grantees to an alternate CLA if a CLA is removed and seek comment on the best process details for effectuating such a transfer.

INITIAL REGULATORY FLEXIBILITY ANALYSIS

As required by the Regulatory Flexibility Act of 1980, as amended (RFA), the Federal Communications Commission (Commission) has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the policies and rules proposed in the *Public Notice* assessing the possible significant economic impact on a substantial number of small entities. The Commission requests written public comments on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments specified on the first page of the *Notice*. The Commission will send a copy of the *Notice*, including this IRFA, to the Chief Counsel for the Small Business Administration (SBA) Office of Advocacy. In addition, the *Notice* and IRFA (or summaries thereof) will be published in the Federal Register.

Need for, and Objectives of, the Proposed Rules. The *IoT Labeling Order* adopted a voluntary cybersecurity labeling program for consumer Internet of Things (IoT) products (U.S. Cyber Trust

Mark (USCTM) Program) that will provide consumers with an easy-to-understand indicator of a product's relative cybersecurity and improve consumer confidence and understanding of IoT product cybersecurity. Under the USCTM Program, authorized products will bear the FCC IoT Label, including the Mark and a QR code that links to easily understandable security-related information about the product. While the Commission retains ultimate control and oversight as the USCTM Program owner, the program is supported by a Lead Administrator and Cybersecurity Label Administrators (CLAs). The Lead Administrator acts as the point of contact between CLAs, which are responsible for certifying use of the FCC IoT Label and the day-to-day management of the program, and the Commission. Further, in collaboration with the CLAs and other stakeholders, the Lead Administrator is required to undertake tasks associated with the launch of the program, including identifying or developing certain recommendations.

In June 2025, the USCTM Lead Administrator, in collaboration with stakeholders (Stakeholder Committee), submitted its recommendations for technical requirements, label requirements, and renewal and surveillance requirements, consistent with the IoT Labeling Order. In April 2026, the Bureau selected the ioXt Alliance (ioXt) to serve as the new Lead Administrator following the prior Lead Administrator's withdrawal. On October 26, 2026, ioXt submitted additional recommendations with respect to technical requirements only, as a result of ongoing stakeholder engagement. The Bureau will seek comment on the technical requirements recommendations in a subsequent Public Notice.

However, in this *Notice*, we seek comment on the *Label Standard* and *Renewal and Surveillance Document*. In particular, we seek comment on the design of the FCC IoT Label, certification renewal processes, and procedures for post-market surveillance and auditing of USCTM-certified products. The Bureau also seeks comment on other related aspects of the program, including procedures to address complaints, non-complying products, and administrator withdrawal or termination. The Commission delegated authority to the Bureau to evaluate the

recommendations and, if the Bureau approves of the recommendations, subject to any required public notice and comment, adopt them into the Commission's rules.

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

Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply. The rules proposed in the *Notice* will apply to small entities in the industries identified in the chart below by their six-digit North American Industry Classification System (NAICS) codes and corresponding SBA size standard. Where available, we also provide additional information regarding the number of potentially affected entities in the industries identified below.

Table 1. 2022 U.S. Census Bureau Data by NAICS Code

Regulated Industry (Footnotes specify potentially affected entities within a regulated industry where applicable)	NAICS Code	SBA Size Standard	Total Firms	Total Small Firms	% Small Firms
Telephone Apparatus Manufacturing	334210	1,250 employees	155	136	87.74%
Radio and Television Broadcasting and Wireless Communications Equip Manufacturing	334220	1,250 employees	155	136	87.74%
Other Communications Equipment Manufacturing	334290	800 employees	310	294	94.84%
Audio and Video Equipment Manufacturing	334310	750 employees	506	492	97.23%
Semiconductor and Related Device Manufacturing	334413	1,250 employees	675	610	90.37%
Wireless Telecommunications Carriers (except Satellite)	517112	1,500 employees	1,184	1,081	91.30%

Regulated Industry (Footnotes specify potentially affected entities within a regulated industry where applicable)	NAICS Code	SBA Size Standard	Total Firms	Total Small Firms	% Small Firms
Other Services Related to Advertising	541890	$19 million	7,067	4,850	68.63%

Table 2. Telecommunications Service Provider Data

2025 Universal Service Monitoring Report Telecommunications Service Provider Data (Data as of December 2024)	SBA Size Standard (1500 Employees)		
Affected Entity	Total # FCC Form 499A Filers	Small Firms	% Small Entities
Wireless Telecommunications *Carriers* (except Satellite)	608	522	85.86
Wireless Telephony	336	262	77.98

Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities. The RFA directs agencies to describe the economic impact of proposed rules on small entities, as well as projected reporting, recordkeeping and other compliance requirements, including an estimate of the classes of small entities which will be subject to the requirements and the type of professional skills necessary for preparation of the report or record.

The USCTM Program will be voluntary, so small entities who do not participate in the program will not be subject to any new or modified reporting, recordkeeping, or other compliance obligations. Small entities that choose to participate in the program will incur recordkeeping, reporting, and other compliance obligations necessary to test their IoT products to demonstrate compliance with the program requirements. Small entities that choose to participate by applying to be a CLA or CyberLAB will also incur recordkeeping, reporting, and other compliance obligations. In this *Notice*, we propose record-related compliance obligations for a Lead Administrator or CLA that intends to withdraw from the program. Specifically, we propose to

require CLAs to provide copies of all records relating to applications and authorization to use the FCC IoT Label, the use of the FCC IoT Label, post-market surveillance, and complaints with respect to rules of the USCTM Program to the Lead Administrator upon request by the Lead Administrator, including but not limited to, when they withdraw from the program and which may be requested before or after the effective date of the CLA's withdrawal. We propose to require each CLA to cooperate with the Lead Administrator with transferring responsibilities to the manufacturer's new CLA of choice, including the transfer of USCTM Program records even if such transfer occurs after the effective date of the CLA's withdrawal. We propose that the records the CLA would be required to transfer to the new CLA include (but would not be limited to) those associated with the CLA's processing of manufacturer applications to include approved, denied, and pending applications; complaints (pending and completed); audits; renewals; and Trademark Use Agreements. We propose to require CLAs to retain these records for a minimum of the term of their Trademark Use Agreement, plus five years thereafter. We also propose to require CLAs to provide the Bureau with a copy of the grantee's records no later than five business days after receiving a request to do so. Administrators will also be required to comply with the timeframes applicable for any federal records as to preservation and disposal of such records.

We propose the same for Lead Administrators, in their capacity as a CLA, including cooperating with the Bureau to transfer responsibilities to a new Lead Administrator, including the transfer of USCTM Program records, even if such transfer occurs after the effective date of the Lead Administrator's withdrawal. We seek comment on these requirements and any additional information that should be provided by outgoing CLAs to new CLAs, as well as any additional actions the outgoing CLA should take for a smooth transition, without interruption to the program.

Discussion of Significant Alternatives Considered That Minimize the Significant Economic Impact on Small Entities. The RFA directs agencies to provide a description of any significant

alternatives to the proposed rules that would accomplish the stated objectives of applicable statutes, and minimize any significant economic impact on small entities. The discussion is required to include alternatives such as: "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities."

For the USCTM Program to be meaningful to consumers, the requirements for an IoT product to be granted authority to use the FCC IoT Label must be uniform for small businesses and other entities. The Bureau maintains the view expressed in the *IoT Labeling Order* that the significance of Mark integrity, and building confidence among consumers that devices and products bearing the FCC IoT Label can be trusted to be cyber secure, necessitates adherence by all entities participating in the program to the same rules, regardless of size. Accordingly, in the *Notice*, the Bureau takes steps to minimize the economic impact on participants in the program of all sizes, including small entities. Specifically, we seek comment on labeling and post-market surveillance requirements, based on recommendations in the *Label Standard* and *Renewal and Surveillance Document*. With respect to the label, we propose to allow manufacturers to print the label directly on product packaging or apply it as an adhesive sticker. We also propose and seek comment on details related to the layout and sizing of the physical label, as well as marketing and advertising of products that bear the label. For each of these proposals, we invite the public, including small businesses, to comment.

Regarding renewal and surveillance, we seek comment on the initial and renewal application information, the renewal period and process, post-market surveillance requirements, and follow-up actions. We propose a three-year renewal cycle to balance consumer protection concerns with the burden on manufacturers and request comment on whether there are modifications or

opportunities to streamline the process that might further reduce burdens on manufacturers, including small entities. We also seek comment on the USCTM "Qualified Professional," that the *Renewal and Surveillance Document* recommends. In particular, we ask whether the expected benefits of such a role outweigh the costs and whether there are alternatives to such a role that may be less costly for manufacturers, many of whom may be small businesses, or whether we should decline to adopt this recommendation. We propose a 90 calendar day deadline for manufacturers to complete renewal evaluations, which we believe provides added flexibility to manufacturers and CLAs and seek comment on this proposal. For post-market surveillance, we seek comment on the format and content of annual reports that CLAs must submit to the Lead Administrator. We invite commenters to make recommendations that minimize the economic impact on CLAs that may be small entities. We also seek comment on post-termination or disqualification procedures that may be more or less burdensome for manufacturers, including small businesses, that fail to comply with program requirements or are otherwise disqualified.

In comments, small entities can identify which of the proposals raised in this *Public Notice* are particularly difficult or costly for them and how different, simplified, or consolidated requirements would address those burdens. They can also propose any modifications to the proposals that would minimize their anticipated economic impact. The Bureau expects to consider more fully the economic impact on small entities following its review of any comments filed in response to the *Public Notice*, including any costs and benefits information we receive. The Bureau's evaluation of the comments filed in this proceeding will shape the final alternatives we consider, the final conclusions we reach, and any final actions we ultimately take in this proceeding to minimize any significant economic impact that may occur on small entities.

Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules. None.

Legal Authority. Sections 1, 2, 4(i), 4(n), 302(a), 303(r), 312, 333, and 503, of the Communications Act of 1934, as amended, 47 U.S.C. 151, 152, 154(i), 154(n), 302a, 303(r), 312, 333, 503 and the IoT Cybersecurity Improvement Act of 2020, 15 U.S.C. 278g-3a to 278g-3e.

List of Subjects in 47 CFR Part 8

Communications, Communications equipment, Computer technology, Consumer protection, Cybersecurity, Electronic products, Internet, Labeling, Laboratories, Marketing agreements, Packaging and containers, Product testing and certification, Printing, Safety, Science and technology, and Telecommunications

Federal Communications Commission**.**

Zenji Nakazawa,
Chief, Public Safety and Homeland Security Bureau.

Proposed Rules

For the reasons discussed in this preamble, the Federal Communications Commission proposes to amend 47 CFR part 8 as follows:

PART 8 – INTERNET TRANSPARENCY FOR CONSUMERS

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

Authority: 47 U.S.C. 151, 152, 154, 201(b), 257, 302a, 303(r), 312, 333, 503 and 1753.

2. Amend § 8.201 by adding paragraphs (d) and (e) to read as follows:

§ 8.201 Incorporation by reference.

* * * * *

(d) ISO/IEC 18004:2024, *Information technology—Automatic identification and data capture techniques—QR Code bar code symbology specification*, Fourth Edition, August 2024; IBR approved for § 8.223.

(e) ISO/IEC 15415:2024, *Automatic identification and data capture techniques—Bar code symbol print quality test specification—Two-dimensional symbols*, Third Edition, December 2024; IBR approved for § 8.223.

3. Amend § 8.203 by adding paragraphs (f)(1) and (2) to read as follows:

§ 8.203 Definitions.

* * * * *

(f) * * *

(1) *Cyber nutrition label*. The format and cybersecurity information specific to the IoT product displayed to the consumer when the QR code is scanned.

(2) *Physical label*. The label that is printed on or adhered to the physical packaging of USCTM-certified products.

* * * * *

4. Amend § 8.208 by revising paragraph (e) and adding paragraph (l) to read as follows:

§ 8.208 Application requirements.

* * * * *

(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 and include:

(1) Applicant's name, address, telephone number(s), email address(es), and website(s);

(2) Contact information for personnel responsible for the application;

(3) Name and address of the agent located in the United States designated by the applicant to receive service of process in the U.S.;

(4) Product name;

(5) Product type; and

(6) The signed technical test report provided by an accredited and recognized CyberLAB.

* * * * *

(l) If an applicant has a pending application with a CLA that is withdrawing or subject to termination, the applicant shall re-file their application with a new CLA of their choice.

5. Amend § 8.216 by revising paragraph (b) to read as follows:

§ 8.216 Termination of authorization to use the FCC IoT Label.

* * * * *

(b) Grant of authorization to use the FCC IoT Label automatically terminates on the certification expiration date for products for which the certification renewal is due, but the grantee does not seek renewal within the timeframe specified in § 8.224(a).

6. Amend § 8.220 by:

a. Revising paragraphs (d)(1) and (e)(5),

b. Adding paragraphs (e)(7) and (8), and

c. Revising paragraph (g)(5).

The revisions and addition read as follows:

§ 8.220 Requirements for CLAs.

* * * * *

(d) * * *

(1) The evaluation of a product, or a portion thereof, may be performed by accredited bodies that meet the applicable requirements of ISO/IEC 17065, in accordance with the applicable provisions of ISO/IEC 17065 for external resources (outsourcing) and other relevant standards. Evaluation is the selection of applicable requirements and the determination that those requirements are met. Evaluation for initial approval to use the FCC IoT Label, renewal certifications, and post-market surveillance may be performed using internal CLA resources or external (outsourced) resources.

(e) * * *

(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. The Lead Administrator will provide written notice to the CLA's authorized manufacturers about the CLA's termination and direct each manufacturer to select a new CLA.

* * * * *

(7) A CLA shall provide 30 days' advance written electronic notice of its intent to withdraw from the program, and the effective date of the withdrawal, to the Chief, Public Safety and Homeland Security Bureau, the Lead Administrator, and the manufacturers it has authorized to use the FCC IoT Label.

(8) A withdrawing CLA shall be required to provide all records relating to applications and authorization to use the FCC IoT Label, the use of the FCC IoT Label, post-market surveillance, and complaints with respect to rules of the FCC IoT Labeling Program to the Lead Administrator upon request by the Lead Administrator and shall cooperate with the Lead Administrator to transfer responsibilities to pending applicants' new CLA of choice, including the transfer of program records, even if such transfer occurs after the effective date of the CLA's withdrawal. These records shall include those associated

with the CLA's processing of manufacturer applications to include approved, denied, and pending applications; complaints (pending and completed); audits; renewals; and Trademark Use Agreements.

* * * * *

(g) * * *

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

* * * * *

7. Amend § 8.221 by revising paragraph (a)(6) and adding paragraph (c) to read as follows:

§ 8.221 Requirements for the Lead Administrator.

(a) * * *

(6) Submit to the Commission annual reports on CLAs' post-market surveillance activities and findings in the format and by the date specified by Public Safety and Homeland Security Bureau;

* * * * *

(c) A Lead Administrator seeking to withdraw from the program as Lead Administrator must provide written electronic notice to the Chief, Public Safety and Homeland Security Bureau, of its intention to withdraw and include the effective date of the withdrawal. The Lead Administrator shall cooperate with the Bureau to transfer responsibilities to a new Lead Administrator, including the transfer of USCTM Program records, even if such transfer occurs after the effective date of the Lead Administrator's withdrawal. These records shall include, but not be limited to, those associated with the Lead Administrator's recognition of CyberLABs to include approved, denied, and pending requests for CyberLAB recognition; complaints (pending and completed); audits; renewals; and Trademark Use Agreements.

8. Amend § 8.222 by revising paragraphs (a) and (b)(10), redesignating paragraph (b)(11) as paragraph (b)(12), and adding new paragraph (b)(11) to read as follows:

§ 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 in English and Spanish in accordance with industry accessibility best practices. 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) * * *

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

(11) Disclosure of camera/video capability, audio capability, and location determination sensors; and

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

9. Add §§ 8.223 through 8.227 to subpart B to read as follows:

§ 8.223 FCC IoT Label

(a) Grantees shall include the FCC IoT (USCTM) Label on their packaging, either printed or using an adhesive label, in accordance with the most current edition of the U.S. Cyber Trust Mark Brand Management Guidelines published by the FCC and available at: www.fcc.gov/CyberTrustMark.

(b) *Sizing*. The FCC IoT (USCTM) Label consisting of the U.S. Cyber Trust Mark image and QR Code shall be no smaller than 1-inch by 2-inches.

(c) *QR Code*. The QR Code shall be comprised of the encoded character string for the URL or other resource identifier of the cyber nutrition label, according to ISO/IEC 18004 (incorporated by reference, see § 8.201).

(1) The QR Code shall range from 21 x 21 modules to 177 x 177 modules, which excludes micro QR sizes, and shall be comprised of modules at least 0.254mm x 0.254mm, according to ISO/IEC 18004 (incorporated by reference, see § 8.201).

(2) The selected module size should be appropriate to the distance, lighting, and typical devices owned by readers, and the QR Code should be surrounded by four (4) modules on all four sides.

(3) The QR Code Quality should meet one of the following: GSI General Specifications or 1.5/(**)/660 where ** is the aperture size best matching the expected reading distance, as per ISO/IEC 15415 (incorporated by reference, see § 8.201).

(d) The cyber nutrition label shall present the required information found in § 8.222(b) of this part. The cyber nutrition label must be available in English and Spanish and designed in accordance with industry accessibility best practices, including ensuring that all information is available via text-to-speech readers. Where the cyber nutrition label links to external websites maintained by the grantee, the grantee must provide the translated text to English and Spanish on those sites.

(e) The FCC IoT Label must be included within the product's online and physical documentation (e.g., user guide).

§ 8.224 Renewal.

(a) Grantees shall seek renewal of each product's USCTM certification every three years. It is the responsibility of the grantee to apply for certification renewal. Grantees should apply to a CLA for renewal at least 90 calendar days prior to the product's certification expiration date and CLAs are required to complete their renewal evaluation within 90 calendar days of receiving the grantee's application.

(b) CLAs must track the renewal due dates of the products they certify; notify the grantee of upcoming renewal deadlines; and notify the Lead Administrator and the Bureau of any products whose certification has automatically terminated due to a failure to renew. The

failure of a CLA to provide notice to a grantee of its upcoming renewal deadline does not excuse the grantee from filing a timely renewal application.

(c) The Grantee's product certification renewal application must include at a minimum:

(1) Grantee's name, address, telephone number(s), email address(es), and website(s);

(2) Contact information for personnel responsible for the renewal application;

(3) Name and address of the agent located in the United States designated by the grantee to receive service of process in the U.S.;

(4) Product name;

(5) Product type;

(6) Date(s) on which each grantee received each authorization to use the Trust Mark;

(7) The authorizing CLA (if different);

(8) A description of changes to the IoT product since it was last evaluated;

(9) A copy of all document(s) related to the granting of authorization to the grantee to use the Trust Mark, including the original application and all CyberLAB report(s); and

(10) A test report conducted by a CyberLAB testing the product against any new or revised USCTM Program requirements and 70% of the remaining requirements (those that are not new or revised).

(d) The CLA shall evaluate the product certification renewal as follows:

(1) Evaluate the product against all new and revised requirements published by the U.S. Cyber Trust Mark program since the product's certification or previous renewal;

(2) Re-evaluate at least 70% of all remaining applicable program requirements (those that are not new or revised) and re-evaluate 100% of all remaining applicable program requirements if at least one instance of non-compliance is found;

(3) Verify that certification for each Backend component that supports the IoT Product is current according to the respective program's validity periods;

(4) Conduct an in-person or remote audit to confirm that the grantee continues to maintain the documents required by § 8.XXX of this part. In addition, review implementation proofs as defined in § 8.XXX of this part performed within the last three months and information regarding the latest security/patch updates shall be provided as verification that processes continue to be implemented.

(5) Confirm the grantee has maintained a U.S. Cyber Trust Mark Qualified Professional for the duration of the grantee's certification period or since the date of last renewal, whichever is more recent.

(d) *USCTM Qualified Professional*. Grantees must notify the CLA who performed the original assessment of any changes to the product or relevant documentation that impact compliance to applicable program requirements. To provide for the consistent identification of compliance-relevant changes, grantee organizations must appoint and maintain a U.S. Cyber Trust Mark Qualified Professional on staff.

(1) The grantee shall appoint the USCTM Qualified Professional(s), ensuring that the designee has obtained, and continues to maintain, appropriate qualifications. If the designated USCTM Qualified Professional leaves the grantee's organizations or is no longer serving in the role, the grantee must notify the CLA(s) that issued the grantee's product certification of the vacancy. The grantee must fill the vacancy for the USCTM Qualified Professional within six months.

(2) To be designated as a grantee organization's USCTM Qualified Professional, the staff member must have:

(i) Completed an approved course on the requirements of the U.S. Cyber Trust Mark Program including the program's scheme requirements;

(ii) Successfully passed the exam associated with the approved course; and

(iii) Confirmed receipt of information from the FCC and the Lead Administrator regarding major changes to the U.S. Cyber Trust Mark program that impact the USCTM Qualified Professional's roles and activities.

(3) To maintain status as a USCTM Qualified Professional an individual shall:

(i) Confirm receipt of information from the FCC and the Lead Administrator regarding major changes to the U.S. Cyber Trust Mark program that impact the USCTM Qualified Professional's role and activities; and

(ii) Repeat course and exam requirements every three years.

Note 1 to paragraph (d)(4): These placeholders are for technical requirements that the Bureau will seek comment on in a subsequent Public Notice.

§ 8.225 Post-Market Surveillance and Ad-Hoc Surveillance.

(a) *Post-Market Surveillance*. CLAs shall apply the following processes to fulfill their post-market surveillance obligations under § 8.220(g).

(1) *Sample Test Plan*. CLAs shall develop a written plan describing how they will ensure that the proper percentage of representative certificated products are tested. CLAs shall submit a Sample Test Plan specific for a given 12-month period to the Lead Administrator annually in September. The Lead Administrator in its role as a CLA will submit its Sample Test Plan to the Bureau annually in September. The Lead Administrator, and the Bureau for the Lead Administrator's Sample Test Plan, will review the Sample Test Plan to ensure it is sufficiently robust to identify and mitigate evolving vulnerabilities throughout a product's life cycle and to ensure consistency among test plans. Lead Administrator will provide CLAs' Sample Test Plan to the Bureau upon request.

(2) *CLA Notification to Grantees*. CLAs shall provide their grantees with a copy of the Lead Administrator approved Sample Test Plan. CLA will also notify grantees in writing that:

(i) CLAs must conduct post-market surveillance sampling.

(ii) The grantee must ensure the availability of production samples at least until the longer of either the end date of the support period communicated on the product registry or no less than one year after the last production date, whichever period is longer.

(iii) The grantee may be required to submit the product for post-market surveillance testing, and that these samples may be requested, at any time, by either the CLA or the Bureau.

(iv) The failure to provide samples within 30 days of the request may result in withdrawal of certification.

(3) *Sample Selection*. Samples audited by a CLA shall be selected from the products certified or renewed by that CLA over the current year or the two-year period directly preceding submission of the sampling plan to the Lead Administrator. A specific product shall only be selected once for audit within its three-year certification period unless requested by the Bureau. When selecting the samples to be audited, a CLA shall prioritize the following:

(i) Broad grantee and laboratory representation;

(ii) Representation of the full range of product types certified;

(iii) Recent security events;

(iv) Representation across the previous four years of certificates issued;

(v) New grantees;

(vi) Grantees with a history of non-compliance; and

(vii) Requests from the Bureau for an audit to be performed on specific product or a group of products.

(4) *Sample Rate, Selection Timeframe, and Report*. A CLA shall adhere to the following sampling, selection, and report requirements:

(i) The total number of products selected for surveillance by a CLA shall be at least three percent of the total number of products certified or renewed by the CLA during the prior calendar year. A "product" is each grant of certification issued.

(ii) When calculating the total number of products to be selected for surveillance, the number of products shall be rounded up to the nearest whole number.

(iii) Products selected for surveillance by the CLA shall be selected from the devices certified or renewed by the CLA over the current calendar year or previous 2 calendar years.

(iv) A product certified in a prior surveillance year, but tested in the present surveillance year, will be credited as surveillance in the present surveillance year.

(v) A CLA must submit an annual report of their post-market surveillance activities for the surveillance year to the Lead Administrator by June 30th of the year following submission of the sampling plan. The post-market surveillance report is for all audits performed by the CLA in the previous calendar year.

(vi) The Bureau may request a specific product or products be subject to post-market surveillance. The CLA may count any such surveillance conducted under a Bureau request toward their annual sampling requirement.

(5) *Obtain Sample.* The CLA shall obtain a sample by the following method:

(i) Request the grantee submit a sample of the certified product either from their latest production line stock or by purchasing a sample of the product from the marketplace for delivery to the CLA or the CLA's designated CyberLAB.

(ii) The CLA shall notify the Lead Administrator if a grantee refuses, or fails to comply with, a request for a sample within 30 days of the CLA request. The Lead Administrator shall notify the Bureau if it is unable to resolve the failure to comply in a reasonable period of time. All grantees shall have received a copy of the Sample Test Plan from the CLA and should be aware that stating that a product is no longer

manufactured or that the product will not be marketed in the United States will not serve as sufficient justification for failing to provide a product sample upon request of the CLA or to the Bureau upon request.

(iii) The grantee shall provide justification to the CLA if it would be overly burdensome for it to keep a production sample on hand or if the production run for the product is limited (i.e., 10 items or fewer). The CLA will determine whether this justification is acceptable and retain this determination within the grantee's record.

(6) *Evaluation*. The sample shall be evaluated by the CLA to determine compliance with the U.S. Cyber Trust Mark program requirements in accordance with the following procedures and requirements:

(i) The CLA shall perform sufficient testing to a provide a high level of confidence that the sample complies with the FCC IoT Labeling Program requirements. Complete testing to all program requirements is not required; however, testing shall be performed on those requirements most likely to be in non-compliance.

(ii) The CLA may perform the testing through either a CLA-run lab or another recognized CyberLAB. In-house manufacturer labs may not be used. Post market surveillance testing should be performed by the same CLA-run lab or CyberLAB that performed the original evaluation whenever possible. The CLA shall inform the grantee of the name of the CLA-run lab or CyberLAB when the sample is obtained.

(iii) The CLA shall compare the test data and sample specifications obtained in the post-market surveillance evaluation with the information submitted in the application filing, verifying consistency. The CLA shall confirm that the grantee has made no changes to the device, applications, or backend/cloud services that impact compliance to the grantee's existing certification to the applicable program requirements. All information shall be consistent.

(iv) [Reserved]

(v) [Reserved]

(vi) The CLA shall examine the sample packaging to determine compliance with the U.S. Cyber Trust Mark program's Labeling requirements.

(vii) The test report documenting surveillance shall be signed by the person(s) performing the tests.

(viii) A review by the certification body personnel shall be made after completion of the evaluation, as to whether the sample complies with the applicable FCC requirements.

(b) *Ad-Hoc Surveillance*. Each CLA shall participate in the ad-hoc surveillance evaluation when initiated by the FCC.

(1) Within 30 days of Bureau initiation, the Lead Administrator will convene a committee consisting of representatives from each CLA, which shall:

(i) Create a decision tree as an objective basis for determining if an ad-hoc surveillance audit is justified (Scope, Logistics Limitations & Risk Model);

(ii) If the Committee determines an audit is not justified, the Lead Administrator will submit the decision tree and its associated justification to the Bureau; and

(iii) If the Committee determines an audit is justified, the Lead Administrator will submit a surveillance plan to the Bureau detailing the types of products to be sampled, the sample rate by CLA, testing to be performed, timeline, and reporting details.

(iv) The Bureau shall be the final arbiter of whether an ad-hoc surveillance audit is conducted.

(2) Once the surveillance plan is approved by Bureau:

(i) Samples shall be obtained as defined in paragraph (a) of this section;

(ii) Evaluation shall be performed in testing facilities as defined in paragraph (a) of this section;

(iii) Reporting shall be created and communicated to the Bureau as described in the Bureau-approved ad-hoc surveillance plan; and

(iv) The Bureau will communicate the ad-hoc surveillance plans to all approved accreditation bodies.

(3) [Reserved]

(c) *Lead Administrator*. The Lead Administrator shall manage post-market surveillance and ad-hoc surveillance for the UCSTM program and carry out the following responsibilities:

(1) Receive annual CLA Sample Test Plans and review them for consistency and compliance with the USCTM program rules and submit its own Sample Test Plan to the Bureau for review;

(2) Convey updates on requirements to the CLAs;

(3) Organize committee of CLA representatives to conduct ad-hoc surveillance;

(4) Reassign post-market surveillance responsibilities in response to changes to CLAs (e.g., CLA withdraws from USCTM Program, conflict of interest);

(5) Monitor and review CLA performance and develop recommendations to the FCC to improve CLA performance (e.g., delays and time to process evaluations, excessive complaints against products tested);

(6) Create and administer the Qualified Professional training and certification, in collaboration with CLAs; and

(7) File annual post-market surveillance, ad hoc and post-audit surveillance reports with the Bureau.

§ 8.226 Complaints.

Complaints can be submitted against U.S. Cyber Trust Mark labeled products to any CLA through their standard complaints management process.

(a) In response to the complaint, the receiving CLA shall notify the Lead Administrator, who will notify the Bureau of the complaint.

(b) The Lead Administrator will determine if the complaint is within the scope of the U.S. Cyber Trust Mark program requirements pursuant to rules adopted by the Commission; confirm the certification status of the product; and assign the complaint to the certifying CLA. The Lead Administrator will notify the Bureau of any product that bears the U.S. Cyber Trust Mark but is not certified. The Commission, via its Public Safety and Homeland Security Bureau, shall resolve any disputes that exceed the functions of the administrator.

(c) The certifying CLA shall follow the procedures outlined in § 8.225(a)(6) (Evaluation).

§ 8.227 Trademark Use and Branding Guidance.

(a) CLAs shall enter into a Trademark Use Agreement and agree to abide by the terms of the USCTM Branding Guidance, which may be updated from time to time at the sole discretion of the agency. The Trademark Use Agreement outlines the rights and expectations of CLAs related to their use of the USCTM and their limited right to authorize certain third-party sub-licensees to use the USCTM, including sub-licensing to authorized manufacturers or other agents, such as advertising agencies, sales agents, and retailers.

(b) CLAs shall maintain complete information about each sub-licensee including (at a minimum) the name, address, telephone number(s), email address(es), and website(s) of each sub-licensee; the date(s) on which each sub-licensee received authorization from the CLA to use any of the licensed marks; the names of any contact personnel for each sub-licensee; and a copy of all document(s) related to the vetting of and granting of the sublicense.

(c) CLAs shall maintain this information for a minimum of the term of the Trademark Use Agreement, plus five years thereafter.

(d) CLAs shall provide the Bureau with these records within five business days of receipt of a request to do so.

(e) CLAs shall provide the Bureau or its designated authorized representatives, with samples and/or relevant documentation regarding any product, commercial item, package, brochure, advertisement, or any other item that has been prepared by or is in the possession of CLA

that the FCC reasonably believes uses, misuses, or incorporates any part or whole of a Cyber Trust Mark.

(f) CLAs shall assist the Bureau in policing unauthorized use of the U.S. Cyber Trust Mark through post-market surveillance and auditing activities, and by notifying the Lead Administrator and FCC as soon as it becomes aware of any use by any other person of a name, trade name, trademark, domain name, email address, metatag, AdWords (or similar search term), mode of advertising, or anything that may reasonably constitute (i) infringement of, (ii) unfair competition with, or (iii) passing off as, any of the Cyber Trust Marks. In addition to promptly reporting the improper usage, the CLAs shall provide relevant material, if available, to the Lead Administrator.

[FR Doc. 2026-23812 Filed: 11/20/2026 8:45 am; Publication Date: 11/23/2026]