Federal Communications Commission
Washington, D.C. 20554

August 14, 2024

DA 24-817

SMALL ENTITY COMPLIANCE GUIDE

Cybersecurity Labeling Program for Internet of Things (IoT) Products
FCC 24-26
PS Docket No. 23-239
Released March 14, 2024

In accordance with the requirements of Section 212 of the Small Business Regulatory Enforcement Fairness Act of 1996, this Small Entity Compliance Guide (Guide) is intended to help small entities—small businesses, small organizations (non-profits), and small governmental jurisdictions—comply with the revised rules adopted in the above-referenced Federal Communications Commission (FCC or Commission) rulemaking dockets. This Guide is not intended to replace or supersede these rules, but to facilitate compliance with the rules. Although we have attempted to cover all parts of the rules that might be especially important to small entities, the coverage may not be exhaustive. This Guide cannot anticipate all situations in which the rules apply. Furthermore, the Commission retains the discretion to adopt case-by-case approaches, where appropriate, that may differ from this Guide. Any decision regarding a particular small entity will be based on the statute and any relevant rules.

In any civil or administrative action against a small entity for a violation of rules, the content of the Guide may be considered as evidence of the reasonableness or appropriateness of proposed fines, penalties or damages. Interested parties are free to file comments regarding this Guide and the appropriateness of its application to a particular situation. The FCC will then consider whether the recommendations or interpretations in the Guide are appropriate in that situation. The FCC may decide to revise this Guide without public notice to reflect changes in the FCC's approach to implementing a rule, or it may clarify or update the text of the Guide. Direct your comments and recommendations, or calls for further assistance, to the FCC's Consumer Center:

1-888-CALL-FCC (1-888-225-5322)
Videophone: 1-844-4-FCC-ASL (1-844-432-2275)
Fax: 1-866-418-0232

TABLE OF CONTENTS

I. OBJECTIVES OF THE PROCEEDING

The *Cybersecurity Labeling for Internet of Things Products Report and Order and Further Notice of Proposed Rulemaking* (*Order*) adopts a voluntary cybersecurity labeling program for wireless Internet of Things (IoT) products. The Federal Communications Commission's (Commission or FCC) IoT Labeling Program (Labeling Program or Program) will provide consumers with an easy-to-understand and quickly recognizable FCC IoT Label that indicates the labeled product meets certain basic minimum cybersecurity requirements. The FCC IoT Label includes a U.S. government certification mark (Cyber Trust Mark) and a QR code that directs consumers to a registry with consumer-friendly information about the security of products bearing the Cyber Trust Mark. The Labeling Program will help consumers make better purchasing decisions, raise consumer confidence with regard to the cybersecurity of IoT products they buy to use in their homes, and encourage manufacturers to develop IoT products with security-by-design principles in mind.

While the IoT Labeling Program will be voluntary, those that choose to participate will be required to ensure their IoT products comply with the Commission's program requirements. These requirements are based on the National Institute of Standards and Technology (NIST) *Profile of the IoT Core Baseline for Consumer IoT Products* (NISTIR 8425). The *Order* focuses the program's scope on wireless consumer IoT products, which includes IoT devices and additional product components necessary to use the IoT product beyond basic operational features, such as a smart speaker or doorbell and the applications used to control them. The Program also focuses on Internet-connected products capable of intentionally emitting radiofrequency energy, relying on the Commission's core Title III authority. Under the oversight of the Commission, qualified Cybersecurity Labeling Administrators (CLAs), including a Lead Administrator selected by the Commission, will be responsible for accepting, reviewing, and approving applications and supporting documentation submitted by entities (e.g., manufacturers) seeking authorization to use the FCC IoT Label. Each application will be supported by testing conducted by an accredited and recognized lab demonstrating the product complies with the Commission's IoT Labeling Program requirements.

The Commission anticipates that as the IoT Labeling Program becomes established in the minds of the consumer, small entities may benefit from recognition of the Cyber Trust Mark on their IoT products, and thus, receive greater recognition in the market as a result of participating in the Program. The Commission adopted a single binary label as proposed in the IoT Labeling NPRM in part due to its simplicity to consumers, but also because small businesses will benefit from a smaller less complex, and likely less costly, labeling design on their product packaging. As noted, the Program is voluntary, and thus, choosing not to participate means that a small business is not obligated to follow any of the associated rules required for Program participants. In adopting this Program, the Commission furthered its goal of providing consumers with reliable information that the IoT products they buy and bring into their homes meet the minimum cybersecurity standards of the Labeling Program, which will strengthen the security of their home products, and the chain of connected IoT products across the larger national IoT ecosystem.

II. COMPLIANCE REQUIREMENTS

The *Order* adds a new subpart to Part 8 of the Commission's rules, establishing a labeling program for consumer IoT products. The rules cover the Program's general provisions, application procedures, authorization conditions, Cybersecurity Label Administrators' requirements and responsibilities, and the IoT registry. A summary of the relevant rules is described below.

A. General Provisions (47 CFR §§ 8.201 – 8.207)

The basis and purpose of the Labeling Program for IoT products is to elevate the nation's cybersecurity posture and provide consumers with assurances regarding their baseline cybersecurity.[1] The Commission adopted definitions relevant to the scope and elements of the Labeling Program,[2] and excluded from the Program all communications equipment on the FCC's Covered List,[3] the Department of Commerce's Entity List,[4] the Department of Defense's List of Chinese Military Companies,[5] and those ineligible for federal procurements or financial awards pursuant to the General Service Administration's System for Award Management.[6] All consumer IoT products produced by these excluded sources are prohibited from obtaining use of the FCC IoT Label. Medical devices regulated by the U.S. Food and Drug Administration, and motor vehicles and motor vehicle equipment regulated by the National Highway Traffic Safety Administration are also excluded from the Program's definition of "Consumer IoT Products."[7]

B. Application Procedures for IoT Product Authorizations (47 CFR §§ 8.208 – 8.212)

1. Applications to certify that a Consumer IoT Product is compliant with the Labeling Program must be signed by the applicant or their authorized agent, and must be submitted in writing to a CLA in the form and format described by the Commission in a public notice to be released by the Public Safety and Homeland Security Bureau (PSHSB or Bureau).

2. Applicants, or their authorized agents, are required to submit an application accompanied by the following information:

a. A written and signed declaration to the CLA that all statements made in the application are true and correct to the best of the applicant's knowledge and belief.

b. A declaration under penalty of perjury that:

i. the Consumer IoT Product for which the applicant is applying for the FCC IoT Label meets all the requirements of the IoT Labeling Program;

---

[1] 47 CFR § 8.201.
[2] 47 CFR § 8.202.
[3] 47 CFR § 8.203(a); *Cybersecurity Labeling Program for Internet of Things*, Report and Order and Further Notice of Proposed Rulemaking, FCC 24-26, at 21, para. 35 (*IoT Labeling Order*). *See* FCC, *List of Equipment and Services Covered By Section 2 of The Secure Networks Act* (Oct. 6, 2023), https://www.fcc.gov/supplychain/coveredlist [https://perma.cc/7EJ4-SDCE].
[4] 47 CFR § 8.203(d); *IoT Labeling Order* at 21, para. 35. *See* Bureau of Industry and Security, U.S. Department of Commerce, Supplement No. 4 to Part 744 – Entity List (2023), https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file [https://perma.cc/STW5-B8GW].
[5] 47 CFR § 8.203(d); *IoT Labeling Order* at 21, para. 35. *See* U.S. Department of Defense, Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. ("Mac") Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283), Tranche 2 (2022), https://media.defense.gov/2022/Oct/05/2003091659/-1/-1/0/1260H%20COMPANIES.PDF [https://perma.cc/5LMA-LZLG].
[6] 47 CFR § 8.203(e); *IoT Labeling Order* at 21, para. 35. *See* U.S. General Services Administration System for Award Management, *Exclusion Types*, https://sam.gov/content/entity-information/resources/exclusion-types [https://perma.cc/5L45-LKCJ] (last visited Feb. 15, 2024).
[7] 47 CFR § 8.202(b); *IoT Labeling Order* at 18-19, para. 32.

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

iii. the product is not comprised of "covered" equipment on the Covered List;

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

v. the product is not owned or controlled by or affiliated with any person or entity that has been suspended or debarred from receiving federal procurements or financial awards, to include all entities and individuals published as ineligible for award on the General Service Administration's System for Award Management as described in § 8.203;

vi. the applicant has taken every reasonable measure to create a securable product;

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

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

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

3. Applicants must also provide a written attestation that they have designated an agent located in the United States (or themselves, if located in the United States) for the purpose of accepting notice of process on behalf of the applicant.

4. A CLA will grant an application to use the FCC IoT Label only if it finds the application is complete, including required test reports, and the Consumer IoT Product complies with the program requirements. Otherwise, an application will be denied.

5. Applications may be dismissed if they are not in accordance with the Commission's rules, the applicant fails to submit additional documents or information upon request, or upon receipt of a written and signed request for dismissal by the applicant or their agent.

6. Any party aggrieved by an action taken by a CLA must first seek review from the CLA within 60 days from the date the CLA issues its decision, and then may seek review from the Commission within 60 days of the CLA's decision on the initial review.

7. A party seeking review of a CLA decision is not authorized to use the FCC IoT Label until the Commission issues a final decision authorizing that use.

C. Authorization Conditions (47 CFR §§ 8.213 – 8.216)

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

2. Using or making reference to the FCC IoT Label or the Cyber Trust Mark in a deceptive or misleading manner in any advertising, brochure, etc. is prohibited.

3. A grantee authorized to use the FCC IoT Label may be required to investigate and respond to complaints received by the Commission concerning their product's potential noncompliance within 20 days.

a. A report submitted in response to such a complaint should also indicate the results of the investigation and what action, if any, has been taken or will be taken to correct the identified defect.

b. In the absence of adequate correction of identified deficiencies, a grantee's authorization to use the FCC IoT will be terminated.

D. CyberLABs (47 CFR §§ 8.217 – 8.218)

1. Applicants seeking a grant of authorization to use the FCC IoT Label must include a compliance test report generated by an accredited and Lead Administrator-recognized testing lab. This can be a third-party lab, an applicant's in-house testing lab, or a CLA-run lab. Third-party labs are referred to as "CyberLABs," and they must demonstrate the following requirements to be recognized by the Commission:

a. Technical expertise in cybersecurity testing and conformity assessment of IoT devices and products;

b. Compliance with accreditation requirements based on the International Organization for Standardization/International Electrotechnical Commission International Standard ISO/IEC 17025;

c. Knowledge of FCC rules and procedures associated with product compliance testing and cybersecurity certification;

d. Necessary equipment, facilities, and personnel to conduct cybersecurity testing and conformity assessment of IoT devices and products;

e. Documented procedures for conformity assessment;

f. Implementation of controls to eliminate potential conflicts of interests, particularly with regard to commercially sensitive information;

g. That the CyberLAB, its affiliates, or subsidiaries are not organizations identified by the listed sources of prohibition under § 8.203; and

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

2. Parties wishing to be recognized by PSHSB as laboratory accreditation bodies must submit a written request to the Chief of PSHSB and provide the following information as evidence of their qualifications:

a. Successful completion of an ISO/IEC 17011 peer review, such as being a signatory to an accreditation agreement that is acceptable to the Commission;

b. Experience with the accreditation of radio and telecommunications testing laboratories to ISO/IEC 17025;

c. Accreditation personnel/assessors with specific technical experience on the Commission cybersecurity certification rules and requirements; and

d. Procedures and policies developed for the accreditation of testing laboratories for FCC cybersecurity certification programs.

3. For a CyberLAB to be recognized by the Lead Administrator, an accreditation body must submit the following information to the Lead Administrator:

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

b. Name of accrediting organization;

c. Scope of laboratory accreditation;

d. Date of expiration of accreditation;

e. Designation number;

f. FCC Registration Number (FRN);

g. A statement as to whether or not the laboratory performs testing on a contract basis;

h. For laboratories outside the United States, details of the arrangement under which the accreditation of the laboratory is recognized; and

i. Other information as requested by the Commission.

E. Cybersecurity Label Administrators (47 CFR §§ 8.219 – 8.221)

1. CLAs will have the following responsibilities, subject to Commission review:

a. Receive and evaluate applications and supporting data for authority to use the FCC IoT Label;

b. Grant authorization to use the FCC IoT Label with a complying consumer IoT product in accordance with the Commission's rules and policies;

c. Accept test data from any Lead Administrator-recognized accredited CyberLAB, subject to the requirements in ISO/IEC 17065, and not unnecessarily repeat tests;

d. Establish and assess fees for processing applications and other Commission-required tasks;

e. Only act on applications that it has received or which it has issued a certification authorizing use of the FCC IoT Label;

f. Dismiss an application that is not in accordance with the provisions adopted, when the applicant requests dismissal, or if the applicant does not submit additional information or test samples requested by the CLA;

g. Ensure that manufacturers make all required information accessible to the IoT registry;

h. Participate in a consumer education campaign in coordination with the Lead Administrator; and

i. Receive complaints alleging an IoT product does not support the cybersecurity criteria conveyed by the Cyber Trust Mark, and refer these complaints to the Lead Administrator, which will notify PSHSB.

2. Additional CLA Responsibilities

a. CLAs will also be responsible for performing appropriate post-market surveillance activities, based on type testing a certain number of samples of the total number of product types for which the CLA has certified use of the FCC IoT Label, and submitting periodic reports of their findings to the Commission;

b. If, during post market surveillance, a CLA determines that a product fails to comply with the technical regulations or other FCC requirements for that product, the CLA shall immediately notify the grantee and the Commission in writing, and the grantee will be required to provide a report to the CLA describing the actions taken to correct the situation, as provided in § 8.216. The CLA must provide a report of these actions to the Commission within 30 days; and

c. CLAs may not make policy, interpret unclear provisions of the statute or rules, or interpret the intent of Congress; grant a waiver of the rules; or take enforcement actions.

d. CLAs may use internal or external (outsourced) resources for evaluation (the selection of applicable requirements and the determination that those requirements are met), but CLAs are prohibited from outsourcing review or application decision activities.

e. When external resources are used for evaluation, including to test products subject to labeling, the CLA shall be responsible for the evaluation and shall maintain appropriate oversight, including periodic audits, of the external resources used to ensure its reliability.

3. CLA Applicants

a. Accredited third parties wishing to become a CLA must file a written application with the Commission which includes:

i. a description of its organization structure,

ii. an explanation of how it will avoid personal and organizational conflict when processing applications,

iii. a description of its processes for evaluating applications seeking authority to use the FCC IoT Label, and

iv. a demonstration of expertise that will be necessary to effectively serve as a CLA including, but not limited to:

a) Cybersecurity expertise and capabilities in addition to industry knowledge of IoT and IoT labeling requirements;

b) Expert knowledge of NIST's cybersecurity guidance, including but not limited to NIST's recommended criteria and labeling program approaches for cybersecurity labeling of Consumer IoT Products;

c) Expert knowledge of FCC rules and procedures associated with product compliance testing and certification;

d) Knowledge of Federal law and guidance governing the security and privacy of agency information systems;

e) Ability to securely handle large volumes of information and demonstration of internal security practices;

f) The CLA applicant must also demonstrate that it is not owned or controlled by or affiliated with any entity identified on the Commission's Covered List or any other listed sources of prohibition under § 8.203; and

g) Implementation of controls to eliminate actual or potential conflicts of interests (including both personal and organizational), particularly with regard to commercially sensitive information.

4. Conditional Commission Approval

    a. To expedite initial deployment of the Labeling Program, the Commission will accept and conditionally approve applications from entities that meet the other FCC program requirements and commit to obtain accreditation pursuant to all the requirements associated with ISO/IEC 17065 with the appropriate scope within six (6) months of when adopted standards and testing procedures become effective.

5. Withdrawal of Commission Approval

    a. The Commission will withdraw its approval of a CLA if the CLA's designation or accreditation is withdrawn, if the Commission determines there is just cause for withdrawing the approval, or upon request of the CLA.

    b. The Commission will also limit the scope of products that can be certified by a CLA if its accreditor limits the scope of its accreditation or if the Commission determines there is good cause to do so.

    c. The Commission will notify a CLA in writing of its intention to withdraw or limit the scope of the CLA's approval and provide at least 60 days for the CLA to respond with an explanation and correction of identified deficiencies.

    d. PSHSB will provide notice to the CLA that that it proposes to terminate the CLA's authority and provide the CLA up to 20 days to respond before reaching a final decision.

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

6. Lead CLA Responsibilities

    a. If more than one qualified entity is selected to be a CLA, the Commission will select a Lead Administrator which will have the following responsibilities, in addition to those required for all CLAs:

        i. Interface with the Commission on behalf of the CLAs, including but not limited to submitting to PSHSB all complaints alleging a product bearing the FCC IoT Label does not meet the requirements of the Commission's Labeling Program;

        ii. Coordinate with CLAs and moderate stakeholder meetings;

        iii. Accept, review, and approve or deny applications from CyberLABs, and maintain a publicly available list of recognized labs, as well as a list of labs that have lost their recognition;

        iv. Within 45 days of publication of updates or changes to NIST guidelines, or adoption by NIST of new guidelines, recommend in collaboration with CLAs and other stakeholders any appropriate modifications to the Labeling Program standards and testing procedures to stay aligned with the NIST guidelines;

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

        vi. Develop in collaboration with stakeholders a consumer education campaign, submit the plan to the Bureau, and participate in consumer education;

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

        viii. Facilitate coordination between CLAs; and

ix. Submit to the Commission any other reports upon request of the Commission or as required by Commission rule.

7. Additional Lead CLA Responsibilities

a. Within 90 days of selection as Lead Administrator, the Lead Administrator will also, in collaboration with stakeholders (e.g. cyber experts from industry, government, and academia), submit the following to PSHSB:

i. Recommendations identifying and/or developing the technical standards and testing procedures for the Commission to consider with regard to at least one class of IoT products eligible for the IoT Labeling Program;

ii. Recommendations on how often a given class of IoT products must renew their request for authority to bear the FCC IoT Label, which may be dependent on the type of product, in connection with the relevant standards recommendations for an IoT product or class of IoT products;

iii. Recommendations on procedures for post-market surveillance by CLAs;

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

v. Recommendations on the design of the FCC IoT Label, including but not limited to labeling design and placement (e.g., size and white spaces, product packaging) and whether to include the product support end date on labels for certain products or category of products.

F. IoT Registry (47 CFR § 8.222)

The *Order* establishes a dynamic, decentralized, publicly accessible registry to be built through a common Application Programming Interface (API) that is secure by design.

1. Grantees authorized to use the FCC IoT Label must make the following information available on the IoT registry:

a. Product Name;

b. Manufacturer name;

c. Date the product received authorization (i.e., cybersecurity certification) to affix the label and current status of the authorization (if applicable);

d. Name and contact information of the CLA that authorized use of the FCC IoT Label;

e. Name of the lab that conducted the conformity testing;

f. Instructions on how to change the default password (specifically state if the default password cannot be changed);

g. Information (or link) for additional information on how to configure the device securely;

h. Information as to whether software updates and patches are automatic and how to access security updates/patches if they are not automatic;

i. The date until which the entity promises to diligently identify critical vulnerabilities in the product and promptly issue software updates correcting them, unless such an update is not reasonably needed to protect against cybersecurity failures (i.e. the minimum

support period); alternatively, a statement that the device is unsupported and that the purchaser should not rely on the manufacturer to release security updates;

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

k. Additional data elements that the Bureau deems necessary.

III. RECORDKEEPING AND REPORTING REQUIREMENTS

The *Order* contains new information collection requirements for manufacturers of consumer IoT products seeking authorization to use the FCC IoT Label. Applicants are required to have their product tested by an accredited and FCC-recognized CyberLAB, Label Administrator Lab, or manufacturer's in-house lab; obtain a report of conformity and compliance from the testing lab; and submit an application for authority to use the Cyber Trust Mark to an FCC-recognized Label Administrator in accordance with procedures established by the Label Administrator. The details and specifics of the reporting and recordkeeping are discussed in Section II of this Guide under the Compliance Requirements.

Additional recordkeeping obligations for Grantees authorized to use the FCC IoT Label require retention of the following records for a two-year period after the marketing of the associated product has been permanently discontinued, or until the conclusion of an investigation or a proceeding if the grantee is officially notified that an investigation or any other administrative proceeding involving its product has been instituted:

1. A record of the original design and specifications and all changes that have been made to the complying consumer IoT product that may affect compliance with the standards and testing procedures established in the Commission's rules;

2. A record of the procedures used for production inspection and testing to ensure conformance with the standards and testing procedures established in the Commission's rules; and

3. A record of the test results that demonstrate compliance with the appropriate regulations for the Labeling Program.

IV. IMPLEMENTATION DATE

The *Order* shall become effective 30 days after publication in the Federal Register, except for the amendments to 47 CFR §§ 8.208, 8.209, 8.212, 8.214, 8.215, 8.217, 8.218, 8.219, 8.220, and 8.221. These amendments may contain new or modified information collection requirements requiring the approval of the Office of Management and Budget (OMB), and will not become effective until OMB has completed review and approval of any new information collection requirements. The Commission will publish a notice in the Federal Register announcing OMB approval, and the relevant effective date(s) of these amendments.

V. INTERNET LINKS

A copy of the *Order* is available at: https://docs.fcc.gov/public/attachments/FCC-24-26A1.pdf.

A copy of the *Order* Erratum is available at: https://docs.fcc.gov/public/attachments/DOC-404300A1_Erratum.docx.