**A.** **Justification**

1. *Circumstances that Make the Information Collection Necessary.*

The Federal Communications Commission (FCC or Commission) is requesting Office of Management and Budget (OMB) approval of a new information collection, which establishes the Commission’s program for cybersecurity labeling for consumer Internet of Things products. The Commission seeks approval of this collection to obtain information from manufacturers filing applications seeking authority to use the label, administrators seeking approval from the Commission to participate in setting up the program and in day-to-day program management, laboratories seeking recognition from the Commission to test consumer IoT products, and the publication of a registry providing additional information on each product authorized to bear the FCC IoT Label. The information collection requested is necessary to establish the FCC’s consumer IoT cybersecurity labeling program, which will provide consumers with easily understood, accessible information on the relative security of a consumer IoT product they are considering for purchase, which will increase the security of devices consumers bring into their homes and as part of a national IoT ecosystem.

On May 12, 2021, Executive Order No. 14028 (EO 14028) was issued, providing various strategies for improving the nation’s cybersecurity posture. Specifically, EO 14028 highlighted the importance of securing the Internet of Things (IoT), and recommended that the Director of the National Institute of Standards and Technology (NIST) initiate “pilot programs informed by existing consumer product labeling programs to educate the public on the security capabilities of Internet-of-Things (IoT) devices.”[[1]](#footnote-3) For these pilot programs, EO 14028 instructed the Director of NIST to identify IoT cybersecurity criteria that reflects increasingly comprehensive levels of testing and assessment for a product to undergo.

In view of these instructions, NIST identified criteria for evaluating the cybersecurity capabilities of IoT consumer devices, informed by existing consumer product labeling programs and input provided by diverse stakeholders.[[2]](#footnote-4) Additionally, NIST published the *Profile of the IoT Core Baseline for Consumer IoT Products (NISTIR 8425)*, identifying cybersecurity capabilities specifically needed in the consumer IoT sector.[[3]](#footnote-5) These efforts from NIST produced baseline product criteria (including both technical product criteria that promotes cybersecurity-related capabilities and non-technical criteria providing important product information),[[4]](#footnote-6) which allowed for the establishment of a conformity assessment program to assess whether a particular IoT product satisfies the baseline product criteria.[[5]](#footnote-7) Further, these efforts allowed for NIST to develop labeling requirements for an IoT product, e.g., a single label indicating that an IoT product has met the baseline product criteria. NIST found that these baseline criteria and labeling requirements would aid consumers in their IoT purchasing decisions by enabling comparisons among IoT products and providing important information about their cybersecurity capabilities.[[6]](#footnote-8)

Building on these efforts by the Executive Office and NIST, and on previous FCC efforts to address IoT,[[7]](#footnote-9) the Commission released a Notice of Proposed Rulemaking (*NPRM*) on August 10, 2023, to address the cybersecurity of consumer IoT products.[[8]](#footnote-10) Specifically, the *NPRM* proposed a voluntary labeling program for IoT that would provide consumers with easily understood, accessible information on the relative security of an IoT device or product.[[9]](#footnote-11) This easily understood and accessible information would be available to the consumer through a label displayed with a complying IoT device or product.

In the *NPRM*, the Commission sought comment on whether the label should be a single label with layering, proposing that one layer contain an FCC IoT mark, while another layer contain a scannable code.[[10]](#footnote-12) Specifically, the FCC IoT Label would indicate that the product or device had met the Commission’s baseline consumer IoT cybersecurity standards, and the scannable code would direct the consumer to more detailed information of the particular IoT product.[[11]](#footnote-13) The Commission also sought comment on where the label should be displayed to best inform consumers.[[12]](#footnote-14) Further, the *NPRM* sought comment on what criteria an IoT device or product should be assessed against and asked whether the criteria established by NIST should be used.[[13]](#footnote-15)

In view of the positive feedback from stakeholders in response to the *NPRM*, the Commission adopted a Report and Order and a Further Notice of Proposed Rulemaking (*Order*) on March 14, 2024.[[14]](#footnote-16) The *Order* established details for compliance with the voluntary program, including the adoption of a single binary label (FCC IoT Label) with layered information.[[15]](#footnote-17) Specifically, the *Order* adopted that the layered information of the FCC IoT Label would include the FCC’s Cyber Trust Mark, an identifiable visual mark indicating that the consumer IoT product has met the Commission’s baseline consumer IoT cybersecurity product.[[16]](#footnote-18) Further, the layered information would include a scannable QR Code, directing the consumer to a decentralized publicly available registry containing more detailed information about the complying IoT product, populated by the manufacturers granted approval to use the FCC IoT Label (grantees) through a common Application Programming Interface (API).[[17]](#footnote-19)

An exemplary image of the U.S. Cyber Trust Mark is shown below.



As discussed in detail in the *Order*, various information is required from entities for participation in the IoT Labeling Program. For example, the process for an entity to receive a grant of authorization to use the FCC IoT Label with their consumer IoT product would entail the entity submitting an application in writing to a Cybersecurity Labeling Administrator (CLA), which certifies that their consumer IoT product is compliant with the IoT Labeling Program.[[18]](#footnote-20) These requirements are adopted as Rule 8.208 of 47 CFR Part 8 by the *Order*. The *Order* also explains how grants of authorization to use the FCC IoT Label are provided to the Commission,[[19]](#footnote-21) adopted as Rule 8.209 by the *Order*. Further, the *Order* outlines how decisions by the CLA can be reviewed by the Commission,[[20]](#footnote-22) adopted as Rule 8.212 by the *Order*.

The *Order* also provides for situations that may arise after a grant of authorization to use the FCC IoT Label has been given. For example, the *Order* provides for mechanisms for review of a manufacturer’s non-compliance regarding a consumer IoT product that has been granted authorization to bear the FCC IoT Label,[[21]](#footnote-23) adopted as Rule 8.214 by the *Order*. Further, the *Order* identifies continuing responsibilities of grantees, including the retention of records,[[22]](#footnote-24) adopted as Rule 8.215 by the *Order*. Additionally, the *Order* enumerates the responsibilities of a grantee with respect to the IoT Registry,[[23]](#footnote-25) adopted as Rule 8.222 by the *Order*.

The *Order* details how an entity receives authority as a CLA, by requiring the entity to file an application with the Commission, including a description of its organization structure, an explanation of how it will avoid personal and organizational conflicts when processing applications, a description of its processes for evaluating applications seeking authority to use the FCC IoT Label, among other information, and a demonstration of expertise that will be necessary to effectively serve as a CLA.[[24]](#footnote-26) These requirements to receive authority as a CLA are adopted as Rules 8.219 and 8.220 of 47 CFR Part 8 by the *Order*. If more than one qualified entity is selected by the Commission to be a CLA, the Commission will select a Lead Administrator from these entities to carry out additional administrative responsibilities.[[25]](#footnote-27) These additional administrative responsibilities are adopted as Rule 8.221 of 47 CFR Part 8 by the *Order*. The *Order* explains that entities seeking to be the Lead Administrator will submit a description of how they will execute the duties of the Lead Administrator. These requirements to receive authority as a Lead Administrator are adopted as Rule 8.221 of 47 CFR Part 8 by the *Order*.

The *Order* details how an entity receives recognition as a testing lab (e.g., CyberLAB, in-house lab) to test and assess IoT products for compliance with the criteria of the IoT Labeling Program. Specifically, the *Order* requires the entity file an application with the Commission, including a description of its organization structure, and a description of its processes for assessing a consumer IoT product, among other requirements.[[26]](#footnote-28) These requirements are adopted as Rule 8.217 of 47 CFR Part 8 by the *Order*. Additionally, the *Order* outlines the ability for an entity to be recognized by the Commission as an accreditation body for testing labs,[[27]](#footnote-29) adopted as Rule 8.218 of 47 CFR Part 8 by the *Order*.

***Information Collection Requirements:***

**§ 8.208 Application requirements.**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(h) If the identified listed sources under § 8.203 are modified after the date of the declaration required by paragraph (b)(6) of this section but prior to grant of authorization to use the FCC IoT Label, then the applicant shall provide a new declaration as required by paragraph (b)(6) of this section.

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

(1) The applicant shall provide a written attestation:

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

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

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

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

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

(k) Signed, as used in this section, means an original handwritten signature or any symbol executed or adopted by the applicant or CLA with the intent that such symbol be a signature, including symbols formed by computer-generated electronic impulses.

Participation in the IoT Labeling Program requires information from an entity seeking a grant of authorization to use the FCC IoT Label in the *Order*. The Commission notes that this collection of information is necessary to determine if their consumer IoT product complies with the IoT Labeling Program requirements. As an example, information such as testing data signed by the person who performed or supervised the tests, will address concerns raised in the record regarding the vigor by which a consumer IoT product was assessed.[[28]](#footnote-30)

**§ 8.209 Grant of authorization to use FCC IoT Label.**

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

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

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

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

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

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

Participation in the IoT Labeling Program requires information from an entity granting authorization to use the FCC IoT Label. The Commission notes that this collection of information is necessary to determine if a consumer IoT product has been determined to comply with the IoT Labeling Program requirements. As an example, information such as showing the effective date of the grant and the CLA granting the authorization, will address concerns raised in the record for maintaining the integrity of the IoT Labeling Program.[[29]](#footnote-31)

**§ 8.212 Review of CLA decisions.**

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

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

(c) Filing deadlines.

(1) An aggrieved party seeking review of a CLA decision by the CLA shall submit such a request within sixty (60) days from the date the CLA issues a decision. Such request shall be deemed submitted when received by the CLA.

(2) An aggrieved party seeking review of a CLA decision by the Commission shall file such a request within sixty (60) days from the date the CLA issues a decision on the party’s request for review. Parties must adhere to the time periods for filing oppositions and replies set forth in 47 CFR § 1.45.

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

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

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

(e) Standard of review.

(1) The PSHSB shall conduct de novo review of request for review of decisions issued by the CLA.

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

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

(1) The Bureau shall, within forty-five (45) days, take action in response to a request for review of a CLA decision that is properly before it. Bureau may extend the time period for taking action on a request for review of a CLA decision for a period of up to ninety days. The Commission may also at any time, extend the time period for taking action of a request for review of a CLA decision pending before the Public Safety and Homeland Security Bureau.

(2) The Commission shall issue a written decision in response to a request for review of a CLA decision that involves novel questions of fact, law, or policy within forty-five (45) days. The Commission may extend the time period for taking action on the request for review of a CLA decision. The Public Safety and Homeland Security Bureau also may extend action on a request for review of a CLA decision for a period of up to ninety days.

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

Participation in the IoT Labeling Program affords an entity seeking a grant of authorization the ability to have a decision by the CLA reviewed by the Commission. The Commission notes that this collection of information is necessary to allow for refinements to the IoT Labeling Program. As an example, information in the request for the review may raise issues not previously considered, thereby suggesting to the Commission future refinements for the IoT Labeling Program.

**§ 8.214 IoT product defect and/or design change.**

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

Participation in the IoT Labeling Program requires continued compliance from the grantee. The Commission notes that this collection of information is necessary to ensure that the IoT Labeling Program requirements are still being adhered to. As an example, information in the report from the grantee may provide information for post market surveillance.

**§ 8.215 Retention of records.**

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

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

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

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

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

Participation in the IoT Labeling Program requires information retention from the grantee. The Commission notes that this collection of information is necessary for audit and post-market surveillance purposes. As an example, information in a record showing test results may establish that a consumer IoT product has the ability to determine that the product is authorized to use the FCC IoT Label. The Commission also notes that these records are likely already kept by the grantee for business purposes, so there is likely no additional burden on the entity outside the scope of their business practices.

**§ 8.217 CyberLABs.**

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

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

(2) Compliance with accreditation requirements based on the International Organization for Standardization/International Electrotechnical Commission International Standard ISO/IEC 17025 (incorporated by reference, see § 8.207).

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

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

(5) Documented procedures for conformity assessment.

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

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

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

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

(c) The Lead Administrator will verify that the CyberLAB is not listed in any of the lists in § 8.203.

(d) The Lead Administrator will maintain a list of accredited CyberLABs that it has recognized, and make publicly available the list of accredited CyberLAB. Inclusion of a CyberLAB on the accredited list does not constitute Commission endorsement of that facility. Recognition afforded to a CyberLAB under the Labeling Program will be automatically terminated for entities that are subsequently placed on the Covered List, listed sources of prohibition under § 8.203, or of it, its affiliate, or subsidiary is owned or controlled by a foreign adversary country defined by the Department of Commerce in 15 CFR § 7.4.

(e) In order to be recognized and included on this list, the accrediting organization must submit the information listed below to the Lead Administrator:

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

(2) Name of accrediting organization;

(3) Scope of laboratory accreditation;

(4) Date of expiration of accreditation;

(5) Designation number;

(6) FCC Registration Number (FRN);

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

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

(9) Other information as requested by the Commission.

(f) [Reserved]

(g) A laboratory that has been accredited with a scope covering the measurements required for the types of IoT products that it will test shall be deemed competent to test and submit test data for IoT products subject to cybersecurity certification. Such a laboratory shall be accredited by a Public Safety and Homeland Security Bureau-recognized accreditation organization based on the International Organization for Standardization/International Electrotechnical Commission International Standard ISO/IEC 17025 (incorporated by reference, see § 8.207). The organization accrediting the laboratory must be recognized by the Public Safety and Homeland Security Bureau to perform such accreditation based on International Standard ISO/IEC 17011 (incorporated by reference, see § 8.207). The frequency for reassessment of the test facility and the information that is required to be filed or retained by the testing party shall comply with the requirements established by the accrediting organization, but shall occur on an interval not to exceed two years.

Participation in the IoT Labeling Program requires information from an entity seeking recognition as a testing lab for the IoT Labeling Program. The Commission notes that this collection of information is necessary for determining the qualifications of an entity seeking recognition. As an example, information such as the name of accrediting organization giving accreditation to the entity seeking recognition is necessary for determining the technical qualifications of the entity.

**§ 8.218 Recognition of CyberLAB accreditation bodies.**

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

(b) Applicants shall provide the following information as evidence of their credentials and qualifications to perform accreditation of laboratories that test equipment to Commission requirements, consistent with the requirements of § 8.217(e). PSHSB may request additional information, or showings, as needed, to determine the applicant’s credentials and qualifications.

(1) Successful completion of an ISO/IEC 17011 (incorporated by reference, see § 8.207) peer review, such as being a signatory to an accreditation agreement that is acceptable to the Commission.

(2) Experience with the accreditation of conformity assessment testing laboratories to ISO/IEC 17025 (incorporated by reference, see § 8.207).

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

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

Participation in the IoT Labeling Program requires information from other entities interested in participating IoT Labeling Program by offering accreditation services. The Commission notes that this collection of information is necessary to determine if an entity has the ability to properly evaluate a testing lab. As an example, information such as the credentials of the entity will allow for PSHSB to determine if the entity is properly suited to grant accreditation for a testing lab.

**§ 8.219 Approval/Recognition of Cybersecurity Label Administrators.**

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

(b) In the United States, the Commission, in accordance with its procedures, allows qualified accrediting bodies to accredit CLAs based on ISO/IEC 17065 (incorporated by reference, see § 8.207) and other qualification criteria. CLAs shall comply with the requirements in § 8.220.

Participation in the IoT Labeling Program requires information from entities seeking recognition as a CLA. The Commission notes that this collection of information is necessary for the Commission to determine which entities have the capabilities of administering aspects of the IoT Labeling Program. As an example, information such as qualifications criteria of an entity allows for determining the capabilities of that entity, and whether these capabilities enable them to be successful in administering the IoT Labeling Program.

**§ 8.220 Requirements for CLAs.**

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

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

(1) A CLA’s methodology for reviewing applications shall be based on type testing as identified in ISO/IEC 17065 (incorporated by reference, *see* § 8.207).

(2) A CLA’s grant of authorization to use the FCC IoT Label shall be based on the application with all the information specified in this part. The CLA shall review the application to determine compliance with the Commission’s requirements and shall issue a grant of product cybersecurity certification in accordance with § 8.208.

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

(1) To be designated as a CLA under this section, an entity shall demonstrate cybersecurity expertise and capabilities in addition to industry knowledge of IoT and IoT labeling requirements.

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

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

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

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

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

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

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

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

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

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

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

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

(1) The Commission will approve as a CLA:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(10) A CLA may not:

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

(ii) Grant a waiver of the rules; or

(iii) Take enforcement actions.

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

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

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

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

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

(5) If during post market surveillance of a complying consumer IoT product, a CLA determines that the product fails to comply with the technical regulations (or other FCC requirements) for that product, the CLA shall immediately notify the grantee and the Commission in writing of its findings. The grantee shall provide a report to the CLA describing the actions taken to correct the situation, as provided in § 8.216, and the CLA shall provide a report of these actions to the Commission within 30 days.

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

Participation in the IoT Labeling Program requires information from entities seeking recognition as a CLA. The Commission notes that this collection of information is necessary for the Commission to determine which entities have the appropriate qualification criteria to administer aspects of the IoT Labeling Program.

**§ 8.221 Requirements for the Lead Administrator.**

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

(1) Interface with the Commission on behalf of the CLAs, including but not limited to submitting to the Bureau all complaints alleging a product bearing the FCC IoT Label does not meet the requirements of the Commission’s labeling program;

(2) Coordinate with CLAs and moderate stakeholder meetings;

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

(4) Within 90 days of election as Lead Administrator, the Lead Administrator will, in collaboration with the CLAs and stakeholders (e.g. cyber experts from industry, government, and academia):

(i) Submit to the Bureau recommendations identifying and/or developing the technical standards and testing procedures for the Commission to consider with regard to at least one class of IoT products eligible for the IoT Labeling Program. The Bureau will evaluate the recommendations, subject to any required public notice and comment, incorporate them by reference into the Commission’s rules;

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

(iii) submit to the Bureau a recommendation on procedures for post market surveillance by the CLAs. The Bureau will evaluate the recommendations, and if the Bureau approves of the recommendations, subject to any required public notice and comment, incorporate them by reference into the Commission’s rules; and

(iv) Submit to the Bureau recommendations on the design of the FCC IoT Label, including but not limited to labeling design and placement (e.g., size and white spaces, product packaging) and whether to include the product support end date on labels for certain products or category of products. The Bureau will evaluate the recommendations, and if the Bureau approves of the recommendations, subject to any required public notice and comment, incorporate them by reference into the Commission’s rules.

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

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

(7) Develop in collaboration with stakeholders a consumer education campaign, submit the plan to the Public Safety and Homeland Security Bureau, and participate in consumer education;

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

(9) Facilitate coordination between CLAs;

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

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

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

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

(i) their previous experience in IoT cybersecurity;

(iii) what role, if any, they have played in IoT labeling;

(iii) their capacity to execute the Lead Administrator duties;

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

(v) a proposed consumer education campaign; and

(vi) additional information the applicant believes demonstrates why they should be the Lead Administrator

(d) [***Reserved***]

Participation in the IoT Labeling Program requires information from entities seeking to be designated as a Lead Administrator. The Commission notes that this collection of information is necessary since a program as intricate as the IoT Labeling Program, will likely have many additional duties that can be addressed by a CLA. As an example, information such as submitting reports to the Commission on post-market surveillance will help to maintain the integrity of the IoT Labeling Program.

**§ 8.222 Establishment of an IoT Registry.**

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

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

(1) Product Name;

(2) Manufacturer name;

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

(4) Name and contact information of the CLA that authorized use of the FCC IoT Label;

(5) Name of the lab that conducted the conformity testing;

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

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

(8) Information as to whether software updates and patches are automatic and how to access security updates/patches if they are not automatic;

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

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

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

Participation in the IoT Labeling Program requires information from entities who have been granted authorization to use the FCC IoT Label. For example, information such as the date a complying consumer IoT product has received authorization will allow consumers to understand how recently a consumer IoT product was evaluated.

The Commission submits that the statutory authority for this collection of information is contained in sections 1, 2, 4(i), 4(n), 302, 303(r), 312, 333, and 503, of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152, 154(i), 154(n), 302a, 303(r), 312, 333, 503; the IoT Cybersecurity Improvement Act of 2020, 15 U.S.C. § 278g-3a to § 278g-3e.

This information collection does not affect individuals or households; thus, there are no impacts under the Privacy Act.

1. *Use of Information.*

The information from the collections authorized by these new Commission rules will allow for manufacturers to submit their products to the IoT Labeling Program. The goal is to implement an IoT Labeling Program that consumers will trust to easily identify and compare consumer IoT products to determine which products meet baseline cybersecurity requirements and are safer than others. The IoT Labeling Program will not guarantee the safety of the products that are successfully labeled, but it will assist consumers in understanding the security risks inherent in certain products. The program will raise consumer confidence with regard to the cybersecurity of the IoT products they purchase. In this way, consumers will have the information necessary to make smart choices without overwhelming them with too much information or difficult to access information. Consumers who purchase an IoT product that bears the FCC IoT Label can be assured that their product meets the minimum cybersecurity standards of the IoT Labeling Program, which in turn will strengthen the chain of connected IoT products in their own homes and as part of a larger national IoT ecosystem.

3*. Technological Collection Techniques.*

The requested information collection can be provided digitally over the Internet (i.e., through websites), or by other forms of electronic media, by the entities desiring to participate in the IoT Labeling Program. An entity seeking authority to be recognized as a CLA will electronically submit documentation to the Commission, which will review the documentation and approve those entities who meet the Commission’s qualifications. CLAs who seek authority as the Lead Administrator will electronically submit additional documentation to the Commission, which will review the documentation and approve the best qualified entity. A manufacturer seeking authority to use the FCC IoT Label will electronically submit documentation including a testing report from an accredited lab, to their chosen CLA, which will review the documentation to determine whether the product meets the Commission’s program requirements. If approved, the manufacturer will be authorized to use the FCC IoT Label with that product. The IoT Label will include the Cyber Trust Mark and a QR Code that links to a decentralized publicly available registry containing information supplied by the manufacturer through a common API. The registry will include and display consumer-friendly information about the security of the product.

4. *Efforts to Identify Duplication*.

The information collection requested is generally not duplicative of any currently existing federal regulatory obligation.[[30]](#footnote-32) While information may be already available to consumers at various locations (on product websites and/or retail locations), the cybersecurity information of an IoT product is not all currently and consistently available in a single location and format that would aid in a consumer’s ability to comparison shop and/or be easily assured of a consumer IoT product’s baseline cybersecurity capabilities. These are the main purposes of the IoT Labeling Program, as helping consumers make informed choices regarding IoT products will advance the Commission’s mission of allowing consumers to understand the cybersecurity capabilities of the IoT products they purchase.[[31]](#footnote-33)

5. *Impact on Small Entities.*

The information collection requested may impact entities seeking participation in the IoT Labeling Program that are small business entities. The Commission is committed to reducing the regulatory burdens on small businesses whenever possible, consistent with the Commission’s other public interest responsibilities. Therefore, pursuant to the *Order*, the Commission’s IoT Labeling Program is completely voluntary. The voluntary nature of the IoT Labeling Program allows for small entities to not be subject to any new or modified reporting, recordkeeping, or other compliance obligations if they choose not to participate in the program. Further, the *Order* has carefully designed and evaluated the reporting requirements to minimize the time and amount of data needed from small entities for the Commission to achieve its objectives as stated in item 1 above.

6. *Consequences if Information is Not Collected.*

The information collection requested is necessary to establish the FCC’s consumer IoT cybersecurity labeling program, which will provide consumers with easily understood, accessible information on the relative security of a consumer IoT product they are considering for purchase and increase the security of devices consumers bring into their homes and as part of a national IoT ecosystem. Further, the information collection requested is necessary to assist consumers with comparison shopping for consumer IoT products. The information collection requested is also necessary to maintain the integrity of the IoT Labeling Program. Information provided by those seeking a grant of authorization to use the FCC IoT Label will be able to have their data recognized in view of an accredited testing lab and identification of non-compliance during post-market surveillance of labeled products, among other aspects, will help maintain the integrity of the program. With continued globalization of consumer product manufacturing and increased use of IoT enabled devices, the Commission in concert with other government agencies, trade associations, and manufacturers is undertaking this effort to reduce the cybersecurity risk to consumers who purchase IoT products. Without this new program, consumers would be much more vulnerable to manufacturers who do not consider consumer safety and cybersecurity vulnerability when manufacturing and marketing their products.

7. *Special Circumstances.*

The information collection is not being conducted in any manner inconsistent with the guidelines of 5 CFR section 1320.

8. *Federal Register Notice; Efforts to Consult with Persons Outside of the Commission*.

On March 26, 2024, pursuant to 5 C.F.R. Section 1320.8(d), a 60-Day Notice was published in the Federal Register (See 89 FR 20964) for the information collection requirements contained in this collection with comments due on or before May 28, 2024. The Commission did not receive any comments following publication of the Notice.

Other than the National Institute of Standards and Technology (NIST), the Cybersecurity and Infrastructure Security Agency (CISA), Food and Drug Administration, Executive Office of the President, the Commission has not consulted with others outside the agency on these collections.

9. *Payments or Gifts to Respondents.*

The Commission does not anticipate providing any payments or gifts to respondents.

10. *Assurances of Confidentiality.*

The Bureau will, on delegated authority issue a Public Notice providing further details on how to apply for authority to use the FCC IoT Label, which will include how to request confidential treatment of submitted information.[[32]](#footnote-34) In addition, the CLAs are required to demonstrate to the Commission that they are able to securely handle large volumes of information and demonstrate internal security practices.[[33]](#footnote-35)

11. *Questions of a Sensitive Nature.*

There are no questions of a sensitive nature with respect to the information collected.

12. *Estimates of the Hour Burden for the Collection of Information.*

The Commission is submitting this as a new information collection, as the collection stems from a novel IoT Labeling Program, which requires that applicants who voluntarily seek to participate in the program provide specific information. The disclosures required under this information collection may need to be updated on occasion. The burden details of this collection for which the Commission seeks approval are described below.

**Annual Burden Hours For Applicants Seeking Authorization to Use the FCC IoT Label:**

1. 47 CFR § 8.208 - Application requirements

The Commission believes there are 100 entities desiring a grant of authorization to use the FCC IoT Label. We anticipate that 100 entities will each file applications for 10 products to use the label. This number is arrived from about 300 responses received in response to the *NPRM*, with over 50+ entities providing multiple responses to the *NPRM*, either individually, or as a large collective. Further, an existing IoT labeling program in Singapore received more than 300 applications requesting assessment for IoT cybersecurity label.[[34]](#footnote-36) If two IoT devices/products per entity were submitted, it would signify that 150 entities are participating in Singapore’s program. Accordingly, the Commission thinks it is fair to assume the middle of the range of the above numbers, thereby arriving at 100 respondents interested in seeking a grant of authorization to use the FCC IoT Label for 10 products each.

**Annual Number of Respondents: 100**

**Annual Number of Responses: 100 respondents x 10 response per respondent = 1,000 responses**

**Annual Burden Hours: 1,000 responses x 10 hours per response = 10,000 hours per respondent annually**

100 respondents x 10 responses x 10 hours = **10,000 Total Burden Hours**

The Commission assumes that respondents generally use “in house” personnel, whose pay is comparable to mid-to-senior level federal employees (GS-12/5, GS-14/5 and GS-15/5). As detailed below, the Commission estimates respondent’s average cost to be $63.49 per hour, using the latest 2024 GS salary figures,[[35]](#footnote-37) to comply with the requirement to submit an application seeking a grant of authorization to use the FCC IoT Label:

Staff Hours Hourly Cost

GS-12/5 Technical Specialist 3 $53.87

GS-12/5 Staff Administrator 3 $53.87

GS-14/5 Engineer 3 $75.70

GS-15/5 Attorney 1 $84.55

**Total Hours and Average Hourly Costs** **10** **$63.49**

**Annual “In-House” Cost:**

10,000 Total Burden Hours x $63.49/hr = **$634,900.00**

1. 47 CFR § 8.212 – Review of CLA decisions

As noted above, the Commission estimates that there are likely approximately 1,000 applications seeking a grant of authorization to use the FCC IoT Label. While specific numbers are not available regarding decision reviews from the existing IoT labeling program in Singapore, the Commission assumes about 5 in 100 consumer IoT product applications may receive a decision from a CLA not granting authorization to use the FCC IoT Label. Of these decisions, the Commission anticipates about half will be brought before the Commission for review, i.e., 1 in 40 applications. If 1,000 applications are anticipated by the Commission, then it is fair to assume that only 25 respondents out of the 1,000 will seek review of a CLA decision.

**Annual Number of Respondents: 25 respondents seeking review**

**Annual Number of Responses: 1 response per respondent (25 responses)**

**Annual Burden Hours: 10 hours per response**

25 respondents x 1 response x 10 hours = **250 Total Burden Hours**

Staff Hours Hourly Cost

GS-12/5 Technical Specialist 1 $53.87

GS-12/5 Staff Administrator 1 $53.87

GS-14/5 Engineer 4 $75.70

GS-15/5 Attorney 4 $84.55

**Total Hours and Average Hourly Costs** **10** **$74.87**

**Annual “In-House” Cost:**

250 Total Burden Hours x $74.87/hr = **$18,717.50**

1. 47 CFR § 8.214 – IoT product defect and/or design change

As noted above, the Commission estimates that there are likely approximately 1,000 applications seeking a grant of authorization to use the FCC IoT Label. While specific numbers are not available regarding complaints filed against respondents who have been granted authorization to use the FCC IoT Label nor for the number of defects found during post-market surveillance from the existing IoT labeling program in Singapore, the Commission assumes about 1 in 100 applications will have a complaint filed against it or be determined to be out of compliance during post-market surveillance. If 1,000 applications are anticipated by the Commission, then only 10 respondents out of the 1,000 will need to respond to a complaint or file a report with the Commission addressing actions they have taken to correct defects found in the course of post-market surveillance.

**Annual Number of Respondents: 10**

**Annual Number of Responses: 1 response per respondent (10 responses)**

**Annual Burden Hours: 20 hours per response**

10 respondent x 1 response x 20 hours = **200 Total Burden Hours**

Staff Hours Hourly Cost

GS-12/5 Technical Specialist 3 $53.87

GS-12/5 Staff Administrator 3 $53.87

GS-14/5 Engineer 6 $75.70

GS-15/5 Attorney 8 $84.55

**Total Hours and Average Hourly Costs** **20** **$72.69**

**Annual “In-House” Cost:**

200 Total Burden Hours x $72.69/hr = **$14,538.00**

1. 47 CFR § 8.215 – Retention of records

The Commission estimates that there will be no burden associated with this collection since the information being collected is information that an entity will likely already collect for standard business purposes, e.g., a record of the original design and specifications and all changes that have been made to the complying consumer IoT product.

0 respondents x 0 response x 0 hours = **0 Total Burden Hours**

1. 47 CFR § 8.222 – Establishment of an IoT Registry

As noted above, the Commission estimates that there are likely around 100 interested respondents who will seek a grant of authorization to use the FCC IoT Label for 10 products each. Even if the Commission generously assumes that all 1,000 applications will receive a grant of authorization to use the FCC IoT Label, complying with this information collection would likely have a minimal burden since the information required by the registry is information already collected by a respondent in their normal course of business operations, e.g., product name, manufacturer name, date of authorizations. Accordingly, only administrative staff would be briefly needed to comply with this information collection. If 1,000 products are anticipated to be approved, and all 1,000 products are assumed to be granted authorization to use the FCC IoT Label, the information to for each of the 1,000 products will need to be included in the registry.

**Annual Number of Respondents: 100**

**Annual Number of Responses: 10 response per respondent (1,000 responses)**

**Annual Burden Hours: 1 hours per response**

100 respondents x 10 responses x 1 hour = **1,000 Total Burden Hours**

Staff Hours Hourly Cost

GS-12/5 Technical Specialist 0 $53.87

GS-12/5 Staff Administrator 1 $53.87

GS-14/5 Engineer 0 $75.70

GS-15/5 Attorney 0 $84.55

**Total Hours and Average Hourly Costs** **1** **$53.87**

**Annual “In-House” Cost:**

1,000 Total Burden Hours x $53.87/hr = **$53,870.00**

Cumulative Totals for the Information Collection for Respondents Seeking a Grant of Authorization to Use the FCC IoT Label:

Total Annual Number of Respondents:100 + 25 + 10 + 0 + 100 respondents **= 235 respondents**

Total Annual Number of Responses:1,000 + 25 + 10 + 0 + 1,000 responses **= 2,035 responses**

Total Annual Burden Hours: 10,000 + 250 + 200 + 0 + 1,000

hours **= 11,450 burden hours**

Total Annual “In-House” Costs: $634,900.00 + $18,717.50 + $14,538.00 + $0 + $53,870.00 = **$722,025.50**

**Annual Burden Hours For Applicants Seeking Recognition as a Cybersecurity Labeling Administrator (CLA) to Administer the IoT Labeling Program:**

1. 47 CFR § 8.219 - Approval/Recognition of Cybersecurity Label Administrators

The Commission believes there are approximately 12 entities desiring recognition as a CLA. This number is arrived from the feedback received in response to the *NPRM*, where over 40 industry organizations provided feedback for the *NPRM*. It is fair to assume that approximately one-third of these industry organizations would be interested in recognition as a CLA, in view of their comments supporting the IoT Labeling Program. For recognition as a CLA, an entity would only submit one application.

**Annual Number of Respondents: 12**

**Annual Number of Responses: 1 per respondent (12 responses)**

**Annual Burden Hours: 20 per response**

12 respondents x 1 response x 20 hours = **240 Total Burden Hours**

As noted previously, the Commission assumes that respondents generally use “in house” personnel, whose pay is comparable to mid-to-senior level federal employees (GS-12/5, GS-14/5 and GS-15/5). As detailed below, the Commission estimates respondent’s average cost to be $69.62 per hour, to receive recognition as a CLA from the Commission:

Staff Hours Hourly Cost

GS-12/5 Technical Specialist 4 $53.87

GS-12/5 Staff Administrator 4 $53.87

GS-14/5 Engineer 6 $75.70

GS-15/5 Attorney 6 $84.55

**Total Hours and Average Hourly Costs 20 $69.62**

**Annual “In-House” Cost:**

240 Total Burden Hours x $69.62/hr = **$16,708.80**

1. 47 CFR § 8.220 – Requirements for CLAs

As explained above, the Commission estimates there are approximately 12 entities desiring as a CLA in view of the feedback received for the *NPRM*. This number is arrived from the feedback received in response to the *NPRM*, where over 40 industry organizations provided feedback for the *NPRM*. It is fair to assume that approximately one-third of these industry organizations would be interested in being an authorized CLA, in view of their comments supporting the IoT Labeling Program. To satisfy requirements to be a CLA, an entity would only need to submit information one time to the Commission.

**Annual Number of Respondents: 12**

**Annual Number of Responses: 1 per respondent (12 responses)**

**Annual Burden Hours: 30 per response**

12 respondents x 1 response x 30 hours = **360 Total Burden Hours**

Staff Hours Hourly Cost

GS-12/5 Technical Specialist 5 $53.87

GS-12/5 Staff Administrator 5 $53.87

GS-14/5 Engineer 10 $75.70

GS-15/5 Attorney 10 $84.55

**Total Hours and Average Hourly Costs 30 $71.37**

**Annual “In-House” Cost:**

360 Total Burden Hours x $71.37/hr = **$25,693.20**

1. 47 CFR § 8.220(g) – Post-market surveillance requirements.

The Commission estimates there will be 12 CLAs. This number is arrived from the feedback received in response to the *NPRM*, where over 40 industry organizations provided feedback for the *NPRM*. All 12 CLAs will be required to conduct post-market surveillance of products they have approved to bear the IoT Label and submit to the Commission reports of their findings. Each CLA will be required to test a certain number of samples of the total number of product types for which the CLA has certified use of the Label. We estimate each CLA will be required to test and submit a report on 50 percent of the approximately 84 applications it has approved.

**Annual Number of Respondents: 12**

**Annual Number of Responses: 42 per respondent (42 responses)**

**Annual Burden Hours: 20 per response**

12 respondents x 42 responses x 20 hours = **10,080 Total Burden Hours**

Staff Hours Hourly Cost

GS-12/5 Technical Specialist 4 $53.87

GS-12/5 Staff Administrator 4 $53.87

GS-14/5 Engineer 6 $75.70

GS-15/5 Attorney 6 $84.55

**Total Hours and Average Hourly Costs 20 $69.62**

**Annual “In-House” Cost:**

10,080 Total Burden Hours x $69.62/hr = **$701,769.60**

1. 47 CFR § 8.221 – **Requirements for the Lead Administrator**

Since the Commission estimates there are approximately 12 entities desiring recognition as a CLA, this allows for the Commission to select a Lead Administrator, as outlined in the *Order*.[[36]](#footnote-38) We assume all 12 would seek authority as the Lead Administrator, however, only one Lead Administrator would be needed as the IoT Labeling Program initially focuses on consumer IoT products. To be selected, an entity CLA seeking authority to be a Lead Administrator would only need to submit information one time to the Commission.

**Annual Number of Respondents: 12**

**Annual Number of Responses: 1 per respondent (12 response)**

**Annual Burden Hours: 10 per response**

12 respondents x 1 responses x 10 hours = **120 Total Burden Hours**

Staff Hours Hourly Cost

GS-12/5 Technical Specialist 3 $53.87

GS-12/5 Staff Administrator 3 $53.87

GS-14/5 Engineer 2 $75.70

GS-15/5 Attorney 2 $84.55

**Total Hours and Average Hourly Costs** **10** **$64.36**

**Annual “In-House” Cost:**

120 Total Burden Hours x $64.36/hr = **$7,723.20**

1. 47 CFR § 8.209 – Grant of authorization to use FCC IoT Label

Since the Commission estimates there are approximately 12 CLAs who will examine approximately 1,000 applications seeking a grant of authorization to use the FCC IoT Label, each CLA will need to assess approximately 84 applications.

**Annual Number of Respondents: 12**

**Annual Number of Responses: 84 per respondent (approximately 1,000 responses)**

**Annual Burden Hours: 20 per response**

12 respondents x 84 responses x 20 hours = **20,160 Total Burden Hours**

Staff Hours Hourly Cost

GS-12/5 Technical Specialist 6 $53.87

GS-12/5 Staff Administrator 2 $53.87

GS-14/5 Engineer 8 $75.70

GS-15/5 Attorney 4 $84.55

**Total Hours and Average Hourly Costs 20 $68.74**

**Annual “In-House” Cost:**

20,160 Total Burden Hours x $68.74/hr = **$1,385,798.40**

Cumulative Totals for the Information Collection for Respondents Seeking Recognition as a CLA:

Total Annual Number of Respondents:12 + 12 + 12 + 12 + 12 respondents **= 60 respondents**

Total Annual Number of Responses:12 + 12 + 42 + 12 + 1,000 responses **= 1,078 responses**

Total Annual Burden Hours: 240 + 360 + 10,080 + 120 + 20,160 hours **= 30,960 burden hours**

Total Annual “In-House” Costs: $16,708.80 + $25,693.20 **+** $701,769.60 + $7,723.20 + $1,385,798.40 = **$2,137,693.20**

1. 47 CFR § 8.217 – CyberLABs

The Commission believes there are 12 entities suitable for recognition as a CyberLAB. This number is arrived from numbers found in industry. Specifically, one industry organization indicates there are dozens of authorized IoT testing labs throughout the world.[[37]](#footnote-39) It is fair to assume that approximately one-third of these entities would be interested in recognition as a CyberLAB. For recognition as a CyberLAB, an entity would only need to submit one application.

**Annual Number of Respondents: 12**

**Annual Number of Responses: 1 per respondent (12 responses)**

**Annual Burden Hours: 20 per response**

12 respondents x 1 response x 20 hours = **240 Total Burden Hours**

As noted previously, the Commission assumes that respondents generally use “in house” personnel, whose pay is comparable to mid-to-senior level federal employees (GS-12/5, GS-14/5 and GS-15/5). As detailed below, the Commission estimates respondent’s average cost to be $69.62 per hour, to receive recognition as a CyberLAB:

Staff Hours Hourly Cost

GS-12/5 Technical Specialist 4 $53.87

GS-12/5 Staff Administrator 4 $53.87

GS-14/5 Engineer 6 $75.70

GS-15/5 Attorney 6 $84.55

**Total Hours and Average Hourly Costs** **20** **$69.62**

**Annual “In-House” Cost:**

240 Total Burden Hours x $69.62/hr = **$16,708.80**

1. 47 CFR § 8.218 – Recognition of CyberLAB accreditation bodies

Since the Commission believes there will 5 entities seeking recognition by the Commission as an accrediting body authorized to accredit CyberLABs and CLAs. For recognition as an accreditation body, an entity would only need to submit one application.

**Annual Number of Respondents: 5**

**Annual Number of Responses: 1 per respondent (5 response)**

**Annual Burden Hours: 10 per response**

5 respondents x 1 response x 10 hours = **50 Total Burden Hours**

As noted previously, the Commission assumes that respondents generally use “in house” personnel, whose pay is comparable to mid-to-senior level federal employees (GS-12/5, GS-14/5 and GS-15/5). As detailed below, the Commission estimates respondent’s average cost to be $69.62 per hour, to receive recognition as an accreditation body:

Staff Hours Hourly Cost

GS-12/5 Technical Specialist 2 $53.87

GS-12/5 Staff Administrator 2 $53.87

GS-14/5 Engineer 3 $75.70

GS-15/5 Attorney 3 $84.55

**Total Hours and Average Hourly Costs 10 $69.62**

**Annual “In-House” Cost:**

50 Total Burden Hours x $69.62/hr = **$3,481**

**Cumulative Totals for All Information Collection Requests:**

Total Annual Number of Respondents:235 + 60 + 12 +5 respondents **= 312 respondents**

Total Annual Number of Responses:2,035 + 1,078 + 12 + 5 responses **= 3,130 responses**

Total Annual Burden Hours: 11,450 + 30,960 + 240 + 50 hours **= 42,700 burden hours**

Total Annual “In-House” Costs: $722,025.50 + $2,137,693.20 + $16,708.80 + $3,481.00 = **$2,879,908.50**

13. *Estimates of the Cost Burden of the Collection to Respondents.*

The Commission expects most reporting requirements will be met by respondents’ “in-house” staff as described in Question 12 above. There are no external costs to the respondents.

14. *Estimates of the Cost Burden to the Commission.*

The Commission does not expect to incur costs beyond the normal labor costs for staff.

15. *Program Change or Adjustment.*

As this is a new information collection, there are program changes to the total number of respondents of +312 respondents, total annual responses of +3,130 responses and total annual burden hours of +42,700 hours, due to the adoption of FCC 24-26. These estimates will be added to OMB’s Active Inventory.

No adjustments are being reported.

16. *Collection of Information Whose Results will be Published.*

There are no plans to publish the result of the collection of information.

17. *Display of Expiration Date of OMB Approval of Collection*.

The Commission is not seeking approval to not display the expiration date for OMB approval of the information collection.

18. *Exception to the Certification Statement for Paperwork Reduction Act Submissions.*

There are no exceptions to the Certification Statement.

**B. Collections of Information Employing Statistical Methods**

The Commission does not anticipate that the collection of information will employ any statistical methods.

1. Exec. Order No. 14028, *Improving the Nation’s Cybersecurity*, 86 Fed. Reg. 26633, 26633 (May 12, 2021) (*IoT Executive Order*). [↑](#footnote-ref-3)
2. *See* NIST, *Recommended Criteria for Cybersecurity Labeling for Consumer IoT Products* (Feb. 4, 2022), <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf>; (*NIST Cybersecurity White Paper*) and NIST, *Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software* (May 24, 2022), <https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/cybersecurity-labeling-consumers-0> (*NIST IoT Cybersecurity Criteria for Consumer Labeling Program Overview*). [↑](#footnote-ref-4)
3. NIST, *NISTIR 8425*, *Profile of the IoT Core Baseline for Consumer IoT Products* (Sept. 20, 2022), <https://csrc.nist.gov/publications/detail/nistir/8425/final> (*NISTIR 8425*). [↑](#footnote-ref-5)
4. *See, e.g.*, NIST, *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products* at 3-10 (2022), <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf>; NIST, *Report for the Assistant to the President for National Security Affairs (APNSA) on Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software, A summary review of labeling actions called for by Executive Order (EO) 14028: Improving the Nation’s Cybersecurity* at 4-5 (2022), <https://www.nist.gov/system/files/documents/2022/05/24/Cybersecurity%20Labeling%20for%20Consumers%20under%20Executive%20Order%2014028%20on%20Improving%20the%20Nation%27s%20Cybersecurity%20Report%20%28FINAL%29.pdf> (NIST Summary Report). [↑](#footnote-ref-6)
5. NIST, *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products* at 21 (2022), <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf>. [↑](#footnote-ref-7)
6. *Id.* at 18-19. [↑](#footnote-ref-8)
7. *See* *Spectrum Requirements for the Internet of Things*, ET Docket No. 21-353, Notice of Inquiry, 36 FCC Rcd 14165 (2021); *Supply Chain NOI*, 36 FCC Rcd 10578, (2021); Report and Order, Order, and Further Notice of Proposed Rulemaking, FCC 22-84 (Nov. 11, 2022); *Revision of Part 15 of the Commission’s Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band*, ET Docket No. 13-49, First Report and Order, 29 FCC Rcd 4127, 4143, para. 54 (2014). [↑](#footnote-ref-9)
8. *See Cybersecurity Labeling for Internet of Things*, PS Docket No. 23-239, FCC 23-65, Notice of Proposed Rulemaking (2023) (*IoT Labeling NPRM*). [↑](#footnote-ref-10)
9. *IoT Labeling NPRM* at 1-2, paras. 1-2. [↑](#footnote-ref-11)
10. *IoT Labeling NPRM* at 16, para. 35. [↑](#footnote-ref-12)
11. *Id.* [↑](#footnote-ref-13)
12. *IoT Labeling NPRM* at 16-17, para. 36. [↑](#footnote-ref-14)
13. *IoT Labeling NPRM* at 16, para. 27. [↑](#footnote-ref-15)
14. *See Internet of Things Labeling Program*, PS Docket No. 23-239, FCC 24-26, Report and Order, and Further Notice of Proposed Rulemaking (2024) (*IoT Labeling Program Order*). [↑](#footnote-ref-16)
15. *IoT Labeling Program Order* at 53-55, paras. 106-109. [↑](#footnote-ref-17)
16. *IoT Labeling Program Order* at 53, para. 106. [↑](#footnote-ref-18)
17. *IoT Labeling Program Order* at 57, paras. 111-121. [↑](#footnote-ref-19)
18. *IoT Labeling Program Order* at 46-48, paras. 87-94. [↑](#footnote-ref-20)
19. *IoT Labeling Program Order* at 30-31, para. 55. [↑](#footnote-ref-21)
20. *IoT Labeling Program Order* at 48, paras. 94-95. [↑](#footnote-ref-22)
21. *IoT Labeling Program Order* at 64-65, paras. 125-126. [↑](#footnote-ref-23)
22. *IoT Labeling Program Order* at 64-65, para. 126. [↑](#footnote-ref-24)
23. *IoT Labeling Program Order* at 57-63, paras. 111-121. [↑](#footnote-ref-25)
24. *IoT Labeling Program Order* at 32-37, paras. 59-64. [↑](#footnote-ref-26)
25. *IoT Labeling Program Order* at 25-26, para. 45. [↑](#footnote-ref-27)
26. *IoT Labeling Program Order* at 37-39, paras. 65-71. [↑](#footnote-ref-28)
27. *IoT Labeling Program Order* at 37-38, para. 67. [↑](#footnote-ref-29)
28. *IoT Labeling Program Order* at 43-44, paras. 83-84. [↑](#footnote-ref-30)
29. *IoT Labeling Program Order* at 43-44, paras. 83-84. [↑](#footnote-ref-31)
30. OMB PRA Guide at 42. [↑](#footnote-ref-32)
31. *IoT Labeling Program Order* at 57, para. 111.  [↑](#footnote-ref-33)
32. *IoT Labeling Program Order* at 47-48, para. 93.  [↑](#footnote-ref-34)
33. *IoT Labeling Program Order* at 32, para. 59. [↑](#footnote-ref-35)
34. *See* Press Release, CSA Singapore, Opening Address by Senior Minister of State, Ministry of Communications and Information, Dr Janil Puthucheary at International IOT Security Roundtable 2022 (Oct. 20, 2022), <https://www.csa.gov.sg/News-Events/speeches/2022/opening-address-by-sms-mci-dr-janil-puthucheary-at-iiot-security-roundtable-2022>.  [↑](#footnote-ref-36)
35. OPM, *General Schedule*, <https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/2024/general-schedule> (last visited Mar. 18, 2024). [↑](#footnote-ref-37)
36. *IoT Labeling Program Order* at 25-26, para. 45. [↑](#footnote-ref-38)
37. *See* CTIA, IoT Network Certified, *Test Labs*, <https://iotnetworkcertified.com/test-labs/> (last visited Mar. 18, 2024). [↑](#footnote-ref-39)