



PUBLIC NOTICE

Federal Communications Commission
45 L Street NE
Washington, DC 20554

News Media Information 202-418-0500
Internet: www.fcc.gov
TTY: 888-835-5322

DA 24-617

Released: June 27, 2024

**PUBLIC SAFETY AND HOMELAND SECURITY BUREAU REQUESTS COMMENT ON
IMPLEMENTATION OF THE
CYBERSECURITY LABELING FOR INTERNET OF THINGS PROGRAM**

PS Docket No. 23-239

Comment Date on Section II.B: (30 days after publication in Federal Register)

Comment Date for All Other Sections: (30 days after publication in the Federal Register)

Reply Comment Date for All Other Sections: (45 days after publication in the Federal Register)

TABLE OF CONTENTS

Heading	Paragraph #
I. INTRODUCTION AND BACKGROUND	1
II. DISCUSSION.....	2
A. Format of CLA and Lead Administrator Applications	2
B. FCC Filing Fees for CLA and Lead Administrator Applications	3
C. Bureau Selection of Cybersecurity Label Administrators and the Lead Administrator	11
D. Lead Administrator Expenses Shared Among CLAs	12
E. Lead Administrator Neutrality	13
F. Withdrawal of CLA and Lead Administrator Approval	14
G. Recognition of CyberLABs by Lead Administrator Located Outside the United States	15
H. Complaints	16
I. Confidentiality and Security Requirements	17
J. Registry	20
III. PROCEDURAL MATTERS.....	25
IV. ORDERING CLAUSES.....	34
APPENDIX A – Supplemental Regulatory Flexibility Analysis	
APPENDIX B – Cybersecurity Labeling Administrator Application Form	

I. INTRODUCTION AND BACKGROUND

1. In March 2024, the Federal Communications Commission (FCC or Commission) adopted a *Report and Order and Further Notice of Proposed Rulemaking*¹ establishing the framework for the Commission's voluntary cybersecurity labeling program for consumer wireless Internet of Things (IoT) products (IoT Labeling Program). Recognizing the additional work that would need to be done to implement the framework, the Commission delegated authority to the Public Safety and Homeland Security Bureau (PSHSB or Bureau), in coordination with the Office of the Managing Director (OMD), to seek comment on certain additional items to further the efficient and timely rollout of the program.² Accordingly, with this *Public Notice*, the PSHSB and OMD request comment on: the format of Cybersecurity Label Administrator (CLA) and Lead Administrator applications; filing fees for CLA applications; criteria for selecting CLAs and the Lead Administrator; CLA sharing of Lead Administrator expenses; Lead Administrator neutrality; processes for withdrawal of CLA and Lead Administrator approvals; recognition of CyberLABs outside the United States; complaint processes; confidentiality and security requirements; and the IoT registry.³

II. DISCUSSION

A. Format of CLA and Lead Administrator Applications

2. The *IoT Labeling Order* provides that the Commission will accept applications for entities seeking to qualify as CLAs and those applicants seeking the position of Lead Administrator,⁴ but did not specify the format these applications should take. The Bureau believes that CLA/Lead Administrator applications should be submitted in narrative format via email and seeks comment on this tentative determination and any alternative methods or formats for submission. While the Bureau recognizes the organizational value of a fillable form, the information to be submitted by entities seeking to be a CLA/Lead Administrator seemingly lends itself to a narrative discussion of the qualifications and strengths the applicant possesses to support the FCC's IoT Labeling Program. The Bureau still could re-evaluate the need for a fillable form after it has processed and reviewed the initial CLA/Lead Administrator applications and seek comment on a proposed format for such a form.⁵ We seek comment on these issues.⁶

¹ *Cybersecurity Labeling for Internet of Things*, PS Docket No. 23-239, Report and Order and Further Notice of Proposed Rulemaking, FCC 24-26, (March 15, 2024) (*IoT Labeling Order*).

² *IoT Labeling Order* at 9, para. 13. See e.g., *id.* at 35, para. 61 (delegating authority to PSHSB, in consultation with OIA, to evaluate and establish qualification criteria for entities outside the U.S. to be approved to act as a CLA); *id.* at 36, para. 64 (delegating authority to PSHSB to open the filing window to receive applications for entities seeking recognition as CLA and delegating authority to PSHSB, in consultation with OMD, to take additional actions necessary to preserve the U.S. Cyber Trust Mark under trademark and additional laws). The Commission also delegated authority to the Office of General Counsel (OGC), to the extent necessary, in certain instances. *Id.* at 36, 62, paras. 64, 121.

³ We note that this *Public Notice* is not meant to address all outstanding implementation issues in connection with the IoT Labeling Program; there are additional implementation matters and specific delegations of authority from the *IoT Labeling Order* that the Bureau will be addressing in subsequent public notices.

⁴ *IoT Labeling Order* at 27, 32, 36, paras. 51, 59, 64.

⁵ See Appendix B (Cyber Label Administrator Application Form).

⁶ The Bureau will provide instructions for submission of the CLA/Lead Administrator applications when it issues the public notice to open the application filing window.

B. FCC Filing Fees for CLA and Lead Administrator Applications

3. The *IoT Labeling Order* directs the Bureau, in conjunction with OMD, to adopt procedures and take additional steps, including applicable fees (pursuant to any required public notice and comment), as necessary to ensure compliance with the Communications Act with respect to any rules adopted therein that contemplate the filing of applications directly with the Commission.⁷ Section 8 of the Communications Act requires the Commission to assess and collect application fees to cover the costs of the Commission to process applications.⁸ Although the Commission has assessed and collected application fees pursuant to section 8 of the Communications Act since 1986,⁹ in 2018, Congress modified section 8 of the Communications Act to change the application fee program from a statutory schedule of application fees to a requirement that the Commission update and amend the existing schedule of application fees by rule to recover the costs of the Commission to process applications.¹⁰ Section 8(c) of the Act also requires the Commission to, by rule, amend the application fee schedule if the Commission determines that the schedule requires amendment to ensure that: (1) such fees reflect increases or decreases in the costs of processing applications at the Commission or (2) such schedule reflects the consolidation or addition of new categories of applications.¹¹

4. In the *2020 Application Fee Order*, the Commission explained that in accordance with the RAY BAUM'S Act, application fees are based on the "costs of the Commission to process

⁷ *IoT Labeling Order* at 32, para. 59 & n.217. The *IoT Labeling Order* directs manufacturers to file applications directly with CLAs to use the U.S. Cyber Trust Mark and, as such, those fees are not contemplated in this inquiry. *See id.* at 45, para. 87. *See also id.* at 47, para. 93 (finding that CLAs may charge reasonable fees for their services and to cover the costs of performing administrative duties).

⁸ 47 U.S.C. § 158.

⁹ Consolidated Omnibus Budget Reconciliation Act of 1985, Pub. L. No. 99-272, §§ 5002(e) and (f), 100 Stat. 82, 118-121 (1986). Before that, the Commission had worked to establish application fees, but encountered various challenges to its implementation. *See Establishment of a Fee Collection Program to Implement the Provisions of the Consolidated Omnibus Budget Reconciliation Act of 1985*, Notice of Proposed Rulemaking, 51 Fed. Reg. 25792, paras. 9-20 (July 16, 1986) (brief history of the FCC's application fee program). While the 1986 schedule adopted by Congress was accurate at the time adopted because it was based on cost information provided by the Commission to Congress, the framework did not allow the fee schedule to change as a result of advancements in technology and corresponding changes in Commission procedures and rules. Notably, the Commission was constrained from adding, removing, or otherwise changing the structure or levels of application fees prior to the RAY BAUM'S Act, outside of a ministerial biannual order adopting without notice and comment changes to fees based on the Consumer Price Index.

¹⁰ The Repack Airwaves Yielding Better Access for Users of Modern Services Act of 2018, or the RAY BAUM'S Act of 2018, amended sections 8 and 9 and added section 9A to the Communications Act of 1934, as amended and provided that such provisions would become effective on October 1, 2018. Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, 132 Stat. 1084, Division P – RAY BAUM'S Act of 2018, Title I, § 103 (2018). 47 U.S.C. § 158. Congress provided, however, that application fees in effect prior to the effective date of the new section 8 would remain in effect until the Commission adjusts or amends such fee. RAY BAUM'S Act of 2018, Title I, § 103(d) (uncodified provisions entitled "Transitional Rules").

¹¹ 47 U.S.C. § 158(c); *Amendment of the Schedule of Application Fees Set Forth in Sections 1.1102 through 1.1109 of the Commission's Rules*, Notice of Proposed Rulemaking, 36 FCC Rcd 1618 (2020) (*2020 Application Fee NPRM*); *Amendment of the Schedule of Application Fees Set Forth in Sections 1.1102 through 1.1109 of the Commission's Rules*, MD Docket No. 20-270, Report and Order, 35 FCC Rcd 15089 (2020) (*2020 Application Fee Order*) (the *2020 NPRM* and the *2020 Application Fee Order* collectively explain the statutory changes and the methodology for adopting and maintaining the new schedule of application fees and discussing how it will be maintained) (collectively *2020 Application Fee Proceeding*).

applications.”¹² Specifically, the Commission establishes an application fee based on direct labor costs of processing a particular application, which are calculated “by multiplying an estimate of the number of hours needed for each task, up through first-level supervisory tasks required to process the application, by an estimate of the labor cost per hour for the employee performing the task and by an estimate of the probability that the task needed to be performed.”¹³ In the *2020 Application Fee Order*, the Commission adopted five functional categories of fees: Wireless Licensing Fees, Media Licensing Fees, Equipment Approval Fees, Domestic Service Fees, and International Service Fees.¹⁴

5. The Bureau seeks comment on whether applications filed with the Commission by entities seeking qualification as a CLA or seeking the position of Lead Administrator constitute an application under section 8 of the Act.¹⁵ If so, is there an existing fee category that would cover such applications? If there are no existing fee categories that are applicable, should new application fee categories, “Cybersecurity Label Administrator” and “Lead Administrator,” be established? We seek comment on the legal and factual basis for assessing a fee pursuant to section 8 of the Communications Act on these applications.

6. If we conclude that a filing with the Commission seeking to be a CLA or to be the Lead Administrator constitutes an application under section 8 of the Act, then we must consider the cost of processing such a filing to inform what fee the Commission would charge in connection with such a filing. We note that the agency has narrowly construed the scope of what constitutes processing for applications subject to fees. Applying the Commission’s framework for the costs of processing applications adopted in the *2020 Application Fee Order*, we believe that the processing of CLA applications, including the initial conditional approval and subsequent review required after the CLA notifies the Commission that it has obtained the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17065 accreditation, consists of engineer and engineer supervisory review, and attorney and attorney supervisory review.

7. As detailed below, the Bureau estimates that the time it will take to process each CLA application will be 15 hours and the time it will take to process each Lead Administrator application will be 8 hours. We estimate the labor cost per hour for the various 2024 general schedule pay grades of the employees that process applications based on the current pay table for Washington, DC, at the step 5 level, we estimate overhead costs as 20% of the salary level also per that rule, and we estimate each employee works 2,087 hours in one year. We also round the fee to the nearest \$5.00 increment as required by section 8 as amended.¹⁶ We seek comment on this approach.

8. The Bureau estimates that each CLA application will require 10 hours of engineering review at the GS-15 level, 2 hours of engineering supervisory review at the GS-15 level; 2 hours of attorney application review at the GS-12 level, and 1 hour of attorney supervisory review at the GS-15 level. The estimated total labor costs (including 20% overhead) for the engineering review (GS-15, step

¹² *2020 Application Fee Order* at 3, para. 5; 47 U.S.C. § 158(a).

¹³ *2020 Application Fee Order* at 5, para. 12. The Commission explained why it viewed processing as a limited set of activities for purposes of establishing a fee under section 8 and how its conclusions are bolstered by limitations on review included in the statute. *2020 Application Fee NPRM* at 63, para. 230 & n.204.

¹⁴ *2020 Application Fee Order* at 6-43, paras. 16-135.

¹⁵ 47 U.S.C. § 158(c). Section 8(b)(1) of the Communications Act also requires the Commission, in every even-numbered year, to adjust the schedule of application fees to reflect increases or decreases in the Consumer Price Index (CPI).

¹⁶ 47 CFR § 0.467(a)(2).

5) of each CLA application is \$1,282.20 (12 engineering hours * 106.85 = 1,282.20).¹⁷ The estimated labor costs (including 20% overhead) for the attorney application review (GS-12, step 5) for each CLA application is \$129.28 (2 hours * \$64.64 = \$129.28).¹⁸ The estimated total labor costs (including 20% overhead) for the attorney supervisory review (GS-15, step 5) for each CLA application is \$106.85 (1 hour * 106.85 = 106.85).¹⁹ The total labor costs per CLA application is \$1,518.33 (1,282.20 + 129.28 + 106.85). Based on these hourly rates and the estimated time for processing each CLA application, the Bureau proposes that the filing fee for a CLA application is \$1,520 and we seek comment on this proposal.

9. Some entities seeking to qualify as a CLA may include additional information in their application seeking the position of Lead Administrator, which will similarly require additional engineering and engineering supervisory review, and attorney application and attorney supervisory review. The Bureau estimates that each Lead Administrator application, which occurs after the CLA application has already been reviewed, will require 4 hours of engineering review at the GS-15 level, 1 hour of supervisory engineering review at the GS-15 level, 2 hours of attorney application review at the GS-12 level, and 1 hour of attorney supervisory review at the GS-15 level.

10. We propose that applications for Lead Administrator must include an additional fee of \$770 to cover the FCC's costs of processing Lead Administrator applications. The Bureau seeks comment on this determination. The Bureau estimates that each Lead Administrator application will require 5 hours of engineering application review at the GS-15, step 5 level at an hourly rate of \$106.85 (5 * 106.85 = 534.25), 2 hours of attorney application review at the GS-12, step 5 level at an hour rate of \$64.64 (2 * 64.64 = 129.28) and 1 hour of attorney supervisor review at the GS-15, step 5 level at an hourly rate of \$106.85 (1 * 106.85 = 106.85) for a total of \$770.38 (534.25 + 129.28 + 106.85). The Bureau seeks comment on the estimation of time to process the Lead Administrator applications and the proposed fee for processing the application. Our proposals for processing fees are based on averages. Given that these are new categories of applications, at this time, we do not believe we have a factual basis to assess fees for administrative updates, minor changes or updates to a CLA application, or for entities seeking to withdraw as a CLA. We also do not believe we have a factual basis to assess fees for administrative updates, minor changes, or updates to a Lead Administrator application, or for an entity seeking to withdraw a Lead Administrator. Until we have experience with processing these new types of applications, it would be difficult to calculate identifiable direct costs beyond those included in the calculation of the initial application fee.²⁰ For both the CLA and Lead Administrator applications, we seek comment on whether we have included in our estimates the appropriate steps under the Commission's *2020 Application Fee Order* framework to determine processing costs. If commenters

¹⁷ The annual pay for a GS-15, step 5 in the Washington-Baltimore-Arlington, DC-MD-VA-WV-PA Locality Pay area is \$185,824. Overhead costs are \$37,164.80 (20% * 185,824 = 37,164.80). The hourly rate of a GS-15, Step 5 including overhead costs based on 2,087 annual hours is \$106.85 (185,824 + 37,164.80 = 222,988.80; 222,988.80/ 2,087 hours = 106.85). The Bureau estimates that each CLA application will require 12 hours of engineering review at the GS-15, step 5 level.

¹⁸ The annual pay for a GS-12, step 5 in the Washington-Baltimore-Arlington, DC-MD-VA-WV-PA Locality Pay area is \$112,425. Overhead costs are \$22,485.00 (20% * 112,425 = 22,485). The hourly rate of a GS-12, step 5 including overhead costs based on 2,087 annual hours is \$64.64 (112,425 + 22,485 = 134,910; 134,910/ 2,087 64.64). The Bureau estimates that each CLA application will require 2 hours of attorney review at the GS-12, step 5 level.

¹⁹ The hourly rate of a GS-15, step 5 attorney is the same as the hourly rate of a GS-15, step 5 engineer, which is \$106.85. The Bureau estimates that each CLA application will require 1 hour of attorney review at the GS-15, step 5 level.

²⁰ See *2020 Application Fee Order* at 9, para. 25.

view our estimates to be over or under inclusive, to the extent practicable, commenters should explain their views by including reference to any application fees adopted in the 2020 proceeding that the commenter considers analogous to the CLA and/or Lead Administrator application.

C. Bureau Selection of Cybersecurity Label Administrators and the Lead Administrator

11. The *IoT Labeling Order* provides that the Bureau will release a public notice opening a filing window for the acceptance of CLA applications, which will include an option for CLA applicants to indicate they also seek the role of Lead Administrator.²¹ The *IoT Labeling Order* specifies the expertise and qualifications each applicant for CLA²² and Lead Administrator must demonstrate²³ and delegates to the Bureau the authority to adopt additional criteria and administrative procedures necessary to efficiently select one or more independent, non-governmental entities to act as CLA(s) and Lead Administrator.²⁴ The Bureau seeks comment on whether there are additional areas of expertise or specific requirements a CLA applicant should be required to demonstrate in addition to those listed in the Order.²⁵ The Bureau seeks comment on what additional criteria, if any, the Bureau should take into consideration during the Lead Administrator selection process. What additional criteria would help us ensure that CLA(s) and the Lead Administrator are able to advance the Commission's policy objective to raise consumer confidence with regard to the cybersecurity of consumer wireless IoT products while strengthening the nation's cybersecurity posture? How should the Bureau differentiate between Lead Administrator candidates for selection? Should all selection criteria be weighted the same? If not, which criteria should carry more?

D. Lead Administrator Expenses Shared Among CLAs

12. The *IoT Labeling Order* "expect[ed]" that the Lead Administrator's expenses "in performing its duties on behalf of the program as a whole" will be "shared among CLAs as a whole," but does not provide a mechanism or details for such sharing.²⁶ The Bureau seeks comment on the most effective mechanism for CLAs to share the Lead Administrator's expenses, including whether and how to distinguish costs associated with identified Lead Administrator responsibilities, potential changes in the Lead Administrator, and the timing of reimbursement for such expenses. Commenters should also consider whether and how any cost sharing mechanism might change after the initial rollout of the program, including any rationale for doing so. Alternatively, we seek comment on whether the Lead Administrator is in the best position to propose how costs should be shared among CLAs. To the extent commenters have estimates of the Lead Administrator's expenses, we invite them to share such estimates. In addition, we seek comment on the categories of expenses that should be attributable to the Lead Administrator's responsibilities under this program. What auditing requirements should be required of the Lead Administrator? Are there financial controls, or other controls, the Commission has adopted in the case of other program administrators that it relies on that would be appropriate in this context? We

²¹ *IoT Labeling Order* at 36, para. 64. The Bureau, in coordination with OMD and OGC will review these applications and determine which applications meet the CLA requirements and which CLA applicant best meets the requirements of Lead Administrator. *See id.*

²² *Id.* at 32, para. 59.

²³ *Id.* at 33, para. 59.

²⁴ *Id.* at 36, para. 64.

²⁵ The *IoT Labeling Order* contemplates the acceptance of applications for CLAs located outside the United States after appropriate international agreements or other appropriate prerequisites are in place. *See id.* at 35, para. 61 (delegating authority to the Bureau in consultation with the Office of International Affairs (OIA), to seek comment on additional qualification criteria for such CLAs at that time).

²⁶ *Id.* at 47, para. 93.

note that the *IoT Labeling Order* does not contemplate other funding sources for the Lead Administrator's expenses, beyond sharing "among CLAs as a whole."

E. Lead Administrator Neutrality

13. The Commission recognized the competitive implications of an entity being both the Lead Administrator and a CLA and, as such, delegated authority to the Bureau to review, seek public comment on, and approve/disapprove the Lead Administrator recommendations.²⁷ We seek comment on whether there are safeguards the Bureau might adopt to ensure the stakeholder process remains competitively neutral and the recommendations the Lead Administrator makes to the Commission (*e.g.*, standards and testing criteria and label design) are stakeholder consensus-based and competitively neutral. For example, are there additional or different safeguards the Commission has adopted in the case of other program administrators that it relies on that would be appropriate in this context?²⁸ We seek comment on whether the Bureau should adopt additional safeguards to ensure fulsome and broad stakeholder engagement in this process. Are there other safeguards the Bureau should adopt to ensure the Lead Administrator, who is potentially a competitor of other CLAs, does not have an unfair economic, or other, competitive advantage?

F. Withdrawal of CLA and Lead Administrator Approval

14. The *IoT Labeling Order* provides that the Commission will withdraw its approval of a CLA if the CLA's designation or accreditation is withdrawn, if there is just cause for withdrawing approval, or upon request of the CLA.²⁹ 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.³⁰ The Bureau will announce the withdrawal of a CLA approval by public notice. The *IoT Labeling Order* also delegates authority to the Bureau to "manage changes in the Lead Administrator."³¹ We believe the same processes should be applied to the withdrawal of the Lead Administrator. We seek comment on this tentative determination. The Bureau also seeks comment on steps that should be taken to replace the Lead Administrator. Should a replacement Lead Administrator be chosen by the Bureau from among the remaining accredited and recognized CLAs based on the same criteria and procedures used to select the original Lead Administrator? Should the Commission open a new filing window for CLAs seeking to be Lead Administrator? What other procedures, if any, should the Commission adopt to ensure the efficient replacement of a Lead Administrator? Should the Bureau set a term for the Lead Administrator and at the end of this term open the position up to new applications? If yes, what term is appropriate? Commenters may provide any other additional information that is pertinent to this inquiry.

G. Recognition of CyberLABs by Lead Administrator Located Outside the United States

15. The *IoT Labeling Order* provides that CyberLABs may be located outside the United States provided they are accredited to ISO/IEC 17025 and the FCC's program scope and delegates

²⁷ See *id.* at 32, 36, paras. 58, 64 & n.237 (delegating authority to the Bureau to review Lead Administrator recommendations and recognizing the potential for anticompetitive preferences in recommendations made to the Bureau if a CLA is chosen as Lead Administrator).

²⁸ See, *e.g.*, 47 CFR § 15.715 (white space database administrator); *id.*, part 52, subpart B (numbering administrators); *id.*, part 54, subpart H (universal service administrator); *id.* § 64.623 (TRS administrators); *id.* § 96.63 (spectrum access system administrators).

²⁹ See 47 CFR § 8.220(e)(2).

³⁰ *Id.*

³¹ *IoT Labeling Order* at 27, para. 51.

authority to the Bureau to adopt any additional criteria or procedures necessary with respect to their use.³² We seek comment on whether there are additional procedures or criteria that should be considered when the Lead Administrator recognizes labs located outside the United States. Are there existing international frameworks in other areas that might provide an appropriate model to allow for recognition of a lab located outside of the United States?

H. Complaints

16. The Commission is the ultimate arbiter of complaints submitted, whether directly to the Commission, CLAs, the Lead Administrator, CyberLABs, or any other third-party entity, alleging improper, nonconforming, and/or unauthorized use of the U.S. Cyber Trust Mark. The Commission will actively and diligently enforce the IoT Labeling Program's requirements to maintain the integrity of the FCC IoT Label, the U.S. Cyber Trust Mark, and the program. The *IoT Labeling Order* emphasized that deceptive or misleading use of the FCC IoT Label or U.S. Cyber Trust Mark are prohibited,³³ and set out a 20-day cure period for grantees to investigate complaints of non-compliance and report the results to the Bureau.³⁴ The *IoT Labeling Order* also determined that the Commission and CLAs will receive complaints of noncompliant displays of the Cyber Trust Mark and delegated authority to the Bureau, in coordination with the Consumer and Governmental Affairs Bureau, to determine the process for receiving and responding to complaints.³⁵ The Lead Administrator will receive complaints about the registry and coordinate with manufacturers to resolve any associated technical problems,³⁶ and the Lead Administrator is also responsible for interfacing with the Commission on behalf of CLAs, including as it relates to complaints.³⁷ We seek comment on the specific processes for receiving and responding to complaints associated with the IoT Labeling Program. Should entities file complaints with the Bureau, in addition to submitting them directly to a CLA, including the Lead Administrator? If complaints are filed with the Commission, should complaints associated with grantees that applied for authorization to use the FCC IoT Label be initially referred to the CLA that reviewed the original application for investigation and a determination of whether the application was approved or denied? Should these processes be different if the complaint involves a CyberLAB located outside of the United States? If so, what is the legal basis for these differences? In situations where there is no associated CLA, such as when a product displays the mark without permission, we believe that complaints of fraudulent or deceptive use of the Cyber Trust Mark by those entities that never applied for authorization (i.e., where there is no applicable CLA) should be filed directly with the Commission. We seek comment on this belief. The Commission determined in the *IoT Labeling Order* that a grant of authorization to use the FCC IoT Label is automatically terminated upon notice by the Bureau following submission of a complaint of non-compliance, if that non-compliance has not been adequately corrected or addressed in a report describing actions taken to correct the deficiencies within 20 days.³⁸ We seek comment on what requirements should follow from such a termination of authority.³⁹ Should the Commission adopt disqualification procedures similar to ENERGY

³² *Id.* at 41, para. 78. *See also id.* at 41, para. 77 (noting that the Commission determined that the Lead Administrator will not recognize, for purposes of the IoT Labeling Program, any testing lab that is an entity, its affiliate, or subsidiary owned or controlled by a “foreign adversary” country, as defined by the Department of Commerce’s rule, 15 CFR § 7.4).

³³ 47 CFR § 8.213(b).

³⁴ 47 CFR § 8.214.

³⁵ *IoT Labeling Order* at 64, para. 126.

³⁶ 47 CFR § 8.221(a)(8).

³⁷ 47 CFR § 8.221(a)(1).

³⁸ *IoT Labeling Order* at 65, para. 127.

³⁹ *See id.* at 66, para. 130.

STAR's, which include ceasing shipments of units displaying the label, ceasing the labeling of associated units, removing references to the label from marketing materials, covering or removing labels on noncompliant units within the brand owner's control, and conducting retail store level assessments to identify mislabeled products?⁴⁰

I. Confidentiality and Security Requirements

17. The Bureau anticipates that the manufacturer applications submitted to CLAs will contain commercially sensitive and proprietary information that the manufacturers customarily treat as confidential, including, but not limited to, test reports. The Bureau proposes that these applications should be treated as presumptively confidential and CLAs should be required to maintain this confidentiality. The Bureau seeks comment on this tentative determination. We also seek comment on whether CLA applications submitted to the Commission will likewise contain commercially sensitive and proprietary information that is routinely treated as confidential and thus should be treated as presumptively confidential.⁴¹ Are certain aspects of either of these applications not appropriately treated as presumptively confidential? Are there public interest and/or transparency reasons to make CLA applications and/or Lead Administrator applications publicly available? Should only those CLA applications that are approved be publicly available, while CLA applications that are denied be kept confidential?

18. Information submitted by manufacturers to CLAs, the Lead Administrator, or CyberLABs, in the course of seeking authority to use the FCC IoT Label, including but not limited to applications and test reports, and information submitted to the Lead Administrator by a lab seeking recognition as a CyberLAB (i.e., authorized to conduct conformance testing under the Commission's IoT Labeling Program) are not agency records of the Commission. Only information submitted to the Commission, such as submissions in furtherance of applications by entities seeking authority from the Commission to be a CLA and/or Lead Administrator, are records of the Commission.

19. The Federal Information Security Modernization Act of 2014 (FISMA)⁴² requires, among other things, that each Federal agency provide protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of "information collected or maintained by or on behalf of the agency" and "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency."⁴³ We tentatively conclude that these requirements attach to the Lead Administrator and CLAs, who both collect and maintain information and operate information systems on behalf of the FCC. We seek comment on this tentative conclusion. We note that in the *IoT Labeling Order*, the Commission described that each entity seeking authority to act as a CLA should demonstrate expertise in, among other things, "[f]ederal law and guidance governing the security and privacy of agency information systems,"⁴⁴ which we believe encompasses FISMA and related guidance from the Office of Management and Budget and publications from the National Institute of Standards and Technology (NIST). If these requirements

⁴⁰ See ENERGY STAR, *Disqualification Procedures ENERGY STAR® Products* (Feb. 28, 2018), https://www.energystar.gov/sites/default/files/asset/document/Disqualification_Procedures_0.pdf.

⁴¹ The Bureau has an obligation to publish data maintained by the Commission that would be subject to disclosure under the Freedom of Information Act (FOIA). See *IoT Labeling Order* at 84, para. 173, and the OPEN Government Data Act, Title II of the Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435 (2019), §§ 201-202.

⁴² Pub. L. No. 113-283, 128 Stat. 3073.

⁴³ 44 U.S.C. § 3554(a)(1)(A).

⁴⁴ *IoT Labeling Order* at 32, para. 59

are applicable to the Lead Administrator and CLAs, would they incur additional costs, and if so, what are they? What benefits would attach to FISMA compliance with respect to the confidentiality, integrity, and availability of information and information systems if FISMA and related requirements are applicable to the Lead Administrator and CLAs? Are there additional security requirements the Commission should require of the databases that are used in support of the IoT Labeling Program?

J. Registry

20. The Commission determined in the *IoT Labeling Order* that the FCC IoT Label must include the Cyber Trust Mark and a QR Code that links to a dynamic, decentralized, publicly available registry containing information supplied by entities authorized to use the FCC IoT Label (e.g., manufacturers) through a common Application Programming Interface (API).⁴⁵ The Commission agreed that it should use a third-party to host and manage the registry due to the resources required to establish the registry; determined that the Lead Administrator is in the best position to interface with manufacturers to ensure the smooth operation of the registry; and directed the Lead Administrator to receive and address any technical issues that arise in connection with the registry's API and displaying information from the registry to the consumer when they present the QR Code. Further, as detailed below, the *IoT Labeling Order* envisioned a registry that supports different presentation options.⁴⁶

21. We seek comment on what, if any, registry disclosure fields, in addition to those already required by the *IoT Labeling Order*, would be beneficial to consumers.⁴⁷ Should manufacturers be required to list the sensors contained in the complying product, such as cameras, microphones, and location tracking devices? Should manufacturers be required to disclose what data is collected by those sensors, and whether that data is shared with third parties?⁴⁸ The Commission also recognizes some products/product classes may benefit from additional data elements being disclosed in the registry.⁴⁹ For example, the Commission observed that “the information contained in the registry for a particular IoT product or product class may also depend on the standards and testing procedures adopted for each particular IoT product.”⁵⁰ The Commission also recognized “that some of the information recommended by NIST in its consumer education recommendations... may be valuable for consumers to see in the registry.”⁵¹ Other possible candidates for inclusion identified in the *IoT Labeling Order* included, “manufacturer’s access control protections (e.g., information about passwords, multi-factor authentication), whether or not the data is encrypted while in motion and at rest (including in the home,

⁴⁵ *Id.* at 57, para. 111. The goal of the registry is to assist the public in understanding security-related information about the products that bear the Cyber Trust Mark. *Id.* at 57, para. 113.

⁴⁶ *Id.*

⁴⁷ *See id.* at 57-58, para. 113. The Commission delegated authority to the Bureau to seek comment on the need for additional data fields beyond the baseline of necessary information that must be displayed for an IoT product in the registry which includes: disclosure of product name, manufacturer name, date of authorization, contact information for the CLA and CyberLAB, instructions on how to change the default password, information on how to configure the device securely, information as to whether software updates are automatic and how to access updates if not, the minimum support period, and whether the manufacturer maintains a Hardware Bill of Materials (HBOM) and/or a Software Bill of Materials (SBOM). *Id.* at 61, para. 118.

⁴⁸ Regarding whether to disclose whether data is shared with third parties, commenters should consider security/privacy issues and if data should be replicated; and if the data should be replicated in multiple repositories – by the relevant CLA(s) or vendors, for example – and publicly accessible via a single query point? *See id.* at 62, para. 121.

⁴⁹ *Id.* at 61, para. 118.

⁵⁰ *Id.*

⁵¹ *Id.*

app, and cloud), patch policies, and security or privacy information.”⁵² Are there particular registry data elements that would support the product’s security features for those using assistive technologies? Are there additional registry disclosure fields that are necessary for specific products/product classes, based on those or other considerations and if so, what they should be?

22. The Commission also delegated authority to the Bureau to establish the structure of the registry; and identify the common API and how the API should be structured and used.⁵³ To this end, we seek comment generally on the structure, format, and maintenance of the registry, and how the queried registry data will be displayed to the consumer.⁵⁴ The Bureau believes that the manufacturer would be responsible for their own product data and keeping the data current. We also believe that the data would be hosted by the manufacturers or in partnership with their selected third party and made available through the common API that is secure by design⁵⁵ and seek comment on these tentative determinations. How should the API access be best secured to ensure its integrity and availability? What controls (*e.g.*, rate limits for use of the API) should be required or allowed, and where would those controls best be implemented? How should manufacturers maintain and implement interactions with their product’s data in connection with the API? Should manufacturers be responsible for maintaining and implementing the API in connection with its interactions with the registry data, and if so, how? How should the Commission reduce burdens on manufacturers in supporting the decentralized registry? We seek comment on how often the registry data should be updated and on how costs involved in maintaining the registry should be handled. We invite commenters to provide any other technical information to be considered in establishing the registry.

23. The Bureau seeks comment on its tentative determination that at least three different registry display options may be supported:

- product specific data hosted by the manufacturer or their selected third party;
- vendor data provided for presentation by a commercial retailer; and
- aggregated data provided for presentation of multiple products.

Are these presentation options consistent with the goals of the *IoT Labeling Order* that the registry should enable the display to the consumer of required information about individual products, while providing the flexibility to support the envisioned use cases? Are there other presentation options that we should consider for the display or consumption of registry information in determining the structure and technical details involved with the operation of the registry? Should the registry meet certain performance metrics so that poor user experience does not discourage use? Who is in the best position to manage access to the distributed registry as well as access to the API and the level of access available?

24. The Bureau seeks comment on its tentative determination that there should be a specific aggregated data “landing page”⁵⁶ for the registry, which should be a “.gov” domain to bring the consumer additional trust and validity to the IoT Labeling Program.⁵⁷ The Bureau also seeks comment on the party

⁵² *Id.*

⁵³ *Id.* at 62, para. 121.

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ The “landing page” is envisioned to be a webpage/site that provides search capabilities to aggregate data pulled from the distributed registry and presents data for individual products or multiple products in a common format as prescribed by the *IoT Labeling Order*.

⁵⁷ See also OMB Memorandum M-23-10, *The Registration and Use of .gov Domains in the Federal Government* (Feb. 8, 2023).

that should be responsible for hosting this landing page. Is the Lead Administrator in the best position to host the landing page? What additional costs are involved with this responsibility? What security procedures must be adopted by that third party? Should the landing page meet certain performance metrics so that poor user experience does not discourage use? Are there additional security or privacy requirements arising from Federal law that are applicable to the registry? Should the registry operator(s), as appropriate, be required to implement adequate security, privacy, and availability controls to meet FISMA low/moderate standards, or a commercial equivalent?

III. PROCEDURAL MATTERS

25. *Regulatory Flexibility Act.* The Regulatory Flexibility Act of 1980, as amended (RFA),⁵⁸ requires that an agency prepare a regulatory flexibility analysis for notice and comment rulemakings, unless the agency certifies that “the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities.”⁵⁹ Accordingly, we have prepared a Supplemental Regulatory Flexibility Analysis (Supplemental IRFA) concerning the possible impact of the rule and policy changes contained in this *Public Notice*. The Supplemental IRFA is set forth in Appendix A. Written public comments are requested on the Supplemental IRFA. Comments must have a separate and distinct heading designating them as responses to the Supplemental IRFA and must be filed by the deadlines for comments on the first page of this document.

26. *Paperwork Reduction Act.* The *Public Notice* may contain new or modified information collection(s) subject to the Paperwork Reduction Act of 1995.⁶⁰ All such new or modified information collection requirements will be submitted to OMB for review under section 3507(d) of the PRA. OMB, the general public, and other federal agencies are invited to comment on any new or modified information collection requirements contained in this proceeding. In addition, pursuant to the Small Business Paperwork Relief Act of 2002,⁶¹ we seek specific comment on how we might “further reduce the information collection burden for small business concerns with fewer than 25 employees.”⁶²

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

28. *Ex Parte Rules – Permit but Disclose.* This proceeding shall be treated as a “permit-but-disclose” proceeding in accordance with the Commission’s *ex parte* rules.⁶³ Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter’s written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments,

⁵⁸ See 5 U.S.C. § 603. The RFA, 5 U.S.C. §§ 601–612, was amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

⁵⁹ *Id.*

⁶⁰ Pub. L. No. 104-13.

⁶¹ Pub. L. No. 107-198.

⁶² 44 U.S.C. § 3506(c)(4).

⁶³ *Id.* §§ 1.1200 *et seq.*

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

29. *Comment Period and Filing Procedures.* Interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the FCC's Electronic Comment Filing System (ECFS).

- Commenting parties may file comments in response to this Notice in PS Docket No. 23-239.
- Electronic Filers: Comments may be filed electronically using the Internet by accessing the ECFS: <https://www.fcc.gov/ecfs>. See *Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).
- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing.
- Filings can be sent by hand or messenger delivery, by commercial courier, or by the U.S. Postal Service. **All filings must be addressed to the Secretary, Federal Communications Commission.**
- Hand-delivered or messenger-delivered paper filings for the Commission's Secretary are accepted between 8:00 a.m. and 4:00 p.m. by the FCC's mailing contractor at 9050 Junction Drive, Annapolis Junction, MD 20701. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.
- Commercial courier deliveries (any deliveries not by the U.S. Postal Service) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
- Filings sent by U.S. Postal Service First-Class Mail, Priority Mail, and Priority Mail Express must be sent to 45 L Street NE, Washington, DC 20554.

30. *People with Disabilities.* To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer and Governmental Affairs Bureau at (202) 418-0530(voice), 202-418-0432 (TTY).

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

32. *Digital Equity and Inclusion.* The Commission, as part of its continuing effort to advance digital equity for all,⁶⁴ including people of color, persons with disabilities, persons who live in rural or

⁶⁴ Section 1 of the Communications Act of 1934 as amended provides that the FCC "regulat[es] interstate and foreign commerce in communication by wire and radio so as to make [such service] available, so far as possible, to all the people of the United States, without discrimination on the basis of race, color, religion, national origin, or

(continued....)

Tribal areas, and others who are or have been historically underserved, marginalized, or adversely affected by persistent poverty or inequality, invites comment on any equity-related considerations⁶⁵ and benefits (if any) that may be associated with the proposals and issues discussed herein. Specifically, we seek comment on how our proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility, as well the scope of the Commission's relevant legal authority.

33. *Further Information.* For further information regarding this proceeding, please contact Tara B. Shostek, Attorney Advisor, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau at (202) 418-8130 or Tara.Shostek@fcc.gov.

IV. ORDERING CLAUSES

34. Accordingly, IT IS ORDERED, pursuant to sections 1, 2, 4(i), 4(n), 302, 303(r), 312, 333, and 503, of the Communications Act of 1934, as amended that this *Public Notice* IS HEREBY ADOPTED.

35. IT IS FURTHER ORDERED that the Commission's Office of the Secretary, SHALL SEND a copy of this *Public Notice*, including the Supplemental Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

(Continued from previous page) _____
sex." 47 U.S.C. § 151.

⁶⁵ The term "equity" is used here consistent with Executive Order 13985 as the consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment, such as Black, Latino, and Indigenous and Native American persons, Asian Americans and Pacific Islanders and other persons of color; members of religious minorities; lesbian, gay, bisexual, transgender, and queer (LGBTQ+) persons; persons with disabilities; persons who live in rural areas; and persons otherwise adversely affected by persistent poverty or inequality. *See* Exec. Order No. 13985, 86 Fed. Reg. 7009, Executive Order on Advancing Racial Equity and Support for Underserved Communities Through the Federal Government (January 20, 2021).

APPENDIX A

Supplemental Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),¹ the Bureau has prepared this Supplemental Initial Regulatory Flexibility Analysis (Supplemental IRFA) of the possible significant economic impact on small entities of the policies and rules discussed in the *Public Notice* to supplement the Commission's Initial and Final Regulatory Flexibility Analyses completed in the *IoT Labeling NPRM* released in August 2023,² and the *IoT Labeling Order* released in March 2024.³ Written public comments are requested on this Supplemental IRFA. Comments must be identified as responses to the Supplemental IRFA and must be filed by the same deadline for comments specified on the first page of this *Public Notice*. The Bureau will send a copy of the *Public Notice*, including this Supplemental IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).⁴ In addition, the *Public Notice* and Supplemental IRFA (or summaries thereof) will be published in the *Federal Register*.⁵

2. *Need for, and Objectives of, the Proposed Rules.* The *IoT Labeling Order* adopted a voluntary cybersecurity labeling program for consumer Internet of Things (IoT) products that will provide consumers with an easy-to-understand indicator of a product's relative cybersecurity and improve consumer confidence and understanding of IoT product cybersecurity. The IoT Labeling Program will authorize qualifying IoT products to display the FCC IoT Label, which includes the U.S. Cyber Trust Mark and a QR Code that links to a registry with product-specific consumer-friendly information. The program will adopt standards and testing procedures based on the National Institute of Standards and Technology (NIST) Core Baseline for Consumer IoT Products,⁶ and it will be supported by Cybersecurity Label Administrators (CLAs) and recognized Cybersecurity Testing Laboratories (CyberLABs). A Lead Administrator will be chosen by the Commission from among the CLAs and will be responsible for collaborating with stakeholders to make recommendations including technical cybersecurity standards and testing procedures with which IoT products must comply to be authorized to use the FCC IoT Label, the label design, and a consumer education campaign, to be reviewed by the Commission.

3. In the *IoT Labeling Order*, the Commission delegated authority to the Public Safety and Homeland Security Bureau (Bureau) to seek comment on certain additional items to further the efficient and timely rollout of the program.⁷ This *Public Notice* seeks comment on a number of those items, including the format of CLA and Lead Administrator applications; filing fees for CLA applications; criteria for selecting CLAs and the Lead Administrator; CLA sharing of Lead Administrator expenses; extensions of time to become accredited; Lead Administrator neutrality; complaint processes; and the IoT registry. The proposals considered in this *Public Notice* will contribute to the voluntary IoT Labeling

¹ 5 U.S.C. § 603. The RFA, 5 U.S.C. §§ 601-612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996, Pub. L. No. 104-121, 110 Stat. 857 (1996).

² See *Cybersecurity Labeling for Internet of Things*, PS Docket No. 23-239, Notice of Proposed Rulemaking, FCC 23-65, Appx. B at 35-42, paras. 1-27 (2023) (*IoT Labeling NPRM*).

³ See *Cybersecurity Labeling for Internet of Things*, PS Docket No. 23-239, Report and Order and Further Notice of Proposed Rulemaking, FCC 24-26, Appx. B at 104-112, paras. 1-28 (2024) (*IoT Labeling Order*).

⁴ See 5 U.S.C. § 603(a).

⁵ See *id.*

⁶ NIST, NISTIR 8425, Profile of the IoT Core Baseline for Consumer IoT Products (2022), <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.pdf>.

⁷ See *IoT Labeling Order* at 9, para. 13.

Program and further the Commission's objective to provide better information to consumers about the cybersecurity of the IoT products they use, and bolster the cybersecurity of the nationwide IoT ecosystem.

4. *Legal Basis.* The proposed action is authorized pursuant to sections 1, 2, 4(i), 4(n), 302, 303(r), 312, 333, and 503, of the Communications Act of 1934, as amended.⁸

5. *Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply.* The RFA directs agencies to provide a description and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules and policies, adopted.⁹ The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."¹⁰ In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.¹¹ A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.¹²

6. As noted above, Regulatory Flexibility Analyses were incorporated into the *IoT Labeling NPRM* and the *IoT Labeling Order*. In those analyses, the Commission described in detail the small entities that might be significantly affected. Accordingly, in this *Public Notice*, for the Supplemental IRFA, we incorporate by reference the descriptions and estimates of the number of small entities from the previous Regulatory Flexibility Analyses in the *IoT Labeling NPRM* and the *IoT Labeling Order*.¹³

7. *Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities.* The IoT Labeling Program will be voluntary, so small entities who do not participate in the program will not be subject to any new or modified reporting, recordkeeping, or other compliance obligations. Small entities that choose to participate in the program will incur recordkeeping, reporting, and other compliance obligations necessary to test their IoT products to demonstrate compliance with the program requirements. Small entities that choose to participate by applying to be a CLA or CyberLAB will also incur recordkeeping, reporting, and other compliance obligations. We note that obligations for small entities and other applicants were detailed and adopted by the Commission in the *IoT Labeling Order*. The proposals and discussions in this *Public Notice* seek comment on additional details to the program, including application, selection, and replacement for CLAs and the Lead Administrator as needed, the complaints process, and the registry.

8. Small entities will need to keep the records necessary to demonstrate initial and continued compliance with program requirements, as an IoT product manufacturer or a CLA, including test reports, records related to potential complaint investigations, and data disclosures for the registry, among others. More specifically, small and other grantees of authority to use the FCC IOT Label may also be subject to additional reporting, recordkeeping, and/or other compliance requirements related to the IoT registry in

⁸ 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.

⁹ 5 U.S.C. § 603(b)(3).

¹⁰ *Id.* § 601(6).

¹¹ *Id.* § 601(3) (incorporating by reference the definition of "small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

¹² 15 U.S.C. § 632.

¹³ See *IoT Labeling NPRM*, Appx. B at 35-42, paras. 1-27; *IoT Labeling Order*, Appx. B at 104-112, paras. 1-28.

light of the our inquiry and request for comments in the *Public Notice* on (1) what, if any additional registry disclosure fields would benefit consumers, and (2) whether to require manufacturers to list the sensors contained a complying product, identify what data is collected by those sensors, and disclose whether that data is shared with third parties.

9. The *Public Notice* calculates and proposes that small and other CLA and Lead Administrator applicants be subject to an application filing fee of \$1,520 for CLA Applicants and an additional \$770 for CLA applicants that apply to be a Lead Administrator, to cover the Commission's costs of processing these applications. With regard to other costs that could result from this proceeding, at this time the record does not include sufficient cost information to allow the Bureau to quantify the costs of compliance for small entities, including whether it will be necessary for small entities to hire professionals to comply with the proposals and other matters upon which we seek comment, if adopted. To help the Bureau more fully evaluate the cost of compliance for small entities should its proposals be adopted, in this *Public Notice*, we request comments on the implications of our proposals and whether there are more efficient and less burdensome alternatives (including cost estimates) for the Bureau to consider. We expect the information we received in comments to help the Bureau identify and evaluate relevant matters for small entities, including compliance costs and other burdens that may result from the proposals and inquiries we make in the *Public Notice*.

10. *Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered.* The RFA requires an agency to describe any significant, specifically small businesses, alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): “(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities.”¹⁴

11. For the IoT Labeling Program to be meaningful to consumers, the requirements for an IoT product to be granted authority to use the FCC IoT Label must be uniform for small businesses and other entities. The Bureau maintains the view expressed in the *IoT Labeling Order* that the significance of mark integrity, and building confidence among consumers that devices and products bearing the FCC IoT Label can be trusted to be cyber secure, necessitates adherence by all entities participating in the program to the same rules, regardless of size.

12. In the *Public Notice*, steps taken by the Bureau which should minimize the economic impact for small entities include our decision not to assess fees for administrative updates, minor changes or updates to a CLA application, or for entities seeking to withdraw as a CLA. The Bureau sought comment on the format of CLA and Lead Administrator applications, as well as the fees associated with those applications, and additional areas of expertise or specific requirements a CLA applicant should be required to demonstrate. We also considered and sought comment on other aspects of the Lead Administrator's roles and responsibilities, including the most effective mechanism for CLAs to share in funding the Lead Administrator's expenses, safeguards the Bureau might adopt to ensure Lead Administrator neutrality, and steps to replace the Lead Administrator as needed. Following our conclusion that CLA and Lead Administrator applications are not covered by any existing Commission fee categories and therefore new categories should be established, we alternatively inquired and sought comment on whether, and which existing Commission fee category do CLA and Lead Administrator applications fall within, if any. Additionally, the Bureau considered whether there are additional procedures or criteria that should be considered when recognizing CyberLABs located outside the United

¹⁴ 5 U.S.C. § 603(c)(1)-(4).

States. As stated in the *IoT Labeling Order*, declining to require CyberLABs to be physically located in the U.S. provides more testing lab options for small and other entities. In comments, small entities can identify other requirements or criteria that could minimize the economic impact as IoT product manufacturers submitting applications to a CLA or CyberLAB, or as a prospective CLA or CyberLAB themselves.

13. The Bureau also sought comment on the process for receiving and responding to complaints associated with the program, as well as what requirements should follow from a termination of authority to use the FCC IoT Label due to noncompliance. We asked whether complaints associated with grantees that applied for authorization to use the FCC IoT Label should be initially referred back to the CLA that reviewed the original application. We believe this would be less costly to small entities than going through a separate entity for investigation of complaints. Small entities can also address in comments whether the termination requirements presented would create significant economic impacts and identify alternatives that may reduce those costs.

14. Additionally, the Bureau considered and sought comment in the *Public Notice* on details related to the publicly accessible IoT registry, including additional data disclosure fields, structure and format of the registry, and the Bureau's determination that the registry landing page should be a ".gov" domain. We considered and asked what additional fields would be beneficial to consumers, such as information related to sensors contained in the product and elements that would support users of assistive technologies. We also considered and asked how the common application programming interface (API) that makes manufacturer data available to consumers should be funded and what responsibilities manufacturers should have for maintaining and implementing it. Small entities can specify in comments whether additional aspects of the registry would create significant economic impacts and identify alternatives that may reduce those costs. Regarding the landing page, we asked what additional costs would be associated with hosting such a page. While small entities choosing to participate in the program would have to make required registry data available through the common API, allowing grantees to report information through the API alleviates the need for additional notification requirements which would increase costs for small entities.

15. The Bureau also proposed in the *Public Notice* that manufacturer applications submitted to CLAs, including but not limited to test reports, are presumptively confidential which should benefit small manufacturers, and sought comment on this approach. We tentatively concluded the Lead Administrator and CLAs are required to comply with the Federal Information Security Management Act of 2002 (FISMA),¹⁵ and we sought comment on whether there are additional costs associated with such compliance. In comments, small entities can identify which of these proposals raised in this *Public Notice* are particularly difficult or costly for them and how different, simplified, or consolidated requirements would address those burdens. They can also propose any modifications to the proposals that would their minimize anticipated economic impact. The Bureau expects to consider more fully the economic impact on small entities following its review of any comments filed in response to the *Public Notice*, including any costs and benefits information we receive. The Bureau's evaluation of the comments filed in this proceeding will shape the final alternatives we consider, the final conclusions we reach, and any final actions we ultimately take in this proceeding to minimize any significant economic impact that may occur on small entities.

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

¹⁵ 44 U.S.C. §§ 3541, *et seq.*

APPENDIX B

FEDERAL COMMUNICATIONS COMMISSION

APPLICATION FOR CYBERSECURITY LABELING ADMINISTRATOR AND LEAD ADMINISTRATOR

CYBERSECURITY LABEL ADMINISTRATOR (CLA)

1. Applicant

Name:		Address		
		Street	City	Zip
Point of Contact:	Name	Title	Email	Phone Number

2. Describe Applicant’s organization structure and how this structure supports the Commission’s CLA requirements.

3. Describe the processes Applicant will use to review applications seeking authority to use the FCC IoT Label (based on type testing as identified in ISO/IEC 17065).

4. Describe the safeguards Applicant will implement (or already has in place) to avoid personal and organization conflict when processing applications.

5. Describe in detail Applicant’s expertise in all of the following areas:

- a) Cybersecurity expertise and capabilities. Include a description of Applicant’s knowledge of IoT and FCC 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) Explain how Applicant will securely handle large volumes of information and include Applicant's related internal security practices.

- f) Explain how Applicant will securely handle large volumes of information and include Applicant's related internal security practices.

- g) Status of accreditation pursuant to all the requirements associated with ISO/IEC 17065 and the FCC scope.

- h) Describe the controls Applicant has implemented to eliminate actual or potential conflicts of interests (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.

Check all that apply:

- 6. Applicant is not owned or controlled by or affiliated¹ with any entity identified on the Commission’s Covered List.
- 7. Applicant is not owned or controlled by or affiliated with any listed sources of prohibition under 47 CFR § 8.204.
- 8. Applicant, its affiliate(s), or subsidiary(ies) are not owned or controlled by a foreign adversary country defined by the Department of Commerce in 15 CFR § 7.4.
- 9. Applicant is not owned or controlled by or affiliated with any person or entity that has been suspended or debarred from receiving federal procurements or financial awards.
- 10. Applicant is not otherwise prohibited from participating in the IoT Labeling Program.

If any of the boxes in this section do not apply to Applicant, attach an exhibit explaining the circumstances and demonstrating why Applicant is qualified to be Lead Administrator.

LEAD ADMINISTRATOR

Applicants seeking the role of Lead Administrator must provide all of the information requested below. (Leave the following information blank if not applying for role of Lead Administrator.) In the following section, provide a detailed description of how Applicant will execute the duties of the Lead Administrator and include all of the following:

- 1. Describe Applicant’s previous experience in IoT cybersecurity.

- 2. Describe Applicant’s previous roles, if any, in IoT labeling.

¹ For purposes of the Commission’s IoT labeling program an “affiliate” is defined as “a person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another person. For purposes of this part the term ‘own’ means to own an equity interest (or the equivalent thereof) of more than 10 percent.” See 47 U.S.C. § 153(2).

3. Describe Applicant’s capacity to execute the Lead Administrator duties.

4. Describe Applicant’s plan/approach to interfacing with the Commission on the behalf of CLAs.

5. Describe in detail Applicant’s plan for engaging and collaborating with stakeholders (including other CLAs) to identify or develop FCC recommendations as required by 47 CFR § 8.221.

6. Describe in detail Applicant’s proposed consumer education campaign.

7. Any additional information Applicant believes demonstrates why they should be on how the applicant's qualifications align with the role of Lead Administrator.

--

Information Current and Complete

Information filed with the FCC must be kept current and complete. The Applicant must notify the FCC regarding any substantial and significant changes in the information furnished in the application(s). See 47 CFR § 1.65

Certification Statements

By signing this applicant, the Applicant certifies that all statements and information provided in this application and in any exhibits or attachments are part of this application and are true, complete, correct, and made in good faith.

The Applicant certifies that neither the Applicant nor any other party to the application is subject to a denial of Federal benefits pursuant to § 5301 of the Anti-Drug Abuse Act of 1988, 21 U.S.C. § 862, because of a conviction for possession or distribution of a controlled substance. This certification does not apply to applications filed in services exempted under § 1.2002(c) of the rules, 47 CFR § 1.2002(c). See 47 CFR § 1.2002(b) for the definition of "party to the application" as used in this certification.

The Applicant certifies that it is not in default on any payment for Commission licenses and that it is not delinquent on any non-tax debt owed to any federal agency.

The Applicant certifies that the Applicant and all of the related individuals and entities required to be disclosed on this application are not person(s) who have been, for reasons of national security, barred by any agency of the Federal Government from federal procurement.

Signature

Typed or printed name of Party Authorized to Sign

First Name:	MI:	Last Name	Suffix	Title

Signature	Date

FAILURE TO SIGN THIS APPLICATION MAY RESULT IN DISMISSAL OF THE APPLICATION AND FORFEITURE OF ANY FEES PAID.