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 24-900

September 10, 2024

PUBLIC SAFETY AND HOMELAND SECURITY BUREAU ANNOUNCES 15-BUSINESS DAY FILING WINDOW FOR CYBERSECURITY LABELING ADMINISTRATOR AND LEAD ADMINISTRATOR APPLICATIONS UNDER THE CYBERSECURITY LABELING FOR INTERNET OF THINGS PROGRAM

PS Docket No. 23-239

1. By this Public Notice, the Federal Communications Commission's (FCC or Commission) Public Safety and Homeland Security Bureau (Bureau) announces that the 15-business day filing window for applications from entities seeking designation by the Commission as a Cybersecurity Labeling Administrator (CLA) and Lead Administrator **will open on September 11, 2024 and close October 1, 2024**.[1] The Bureau also provides determinations regarding application format, filing fees, selection criteria, sharing of expenses, Lead Administrator neutrality, and confidentiality and security requirements in this Public Notice.[2]

I. BACKGROUND

2. In March 2024, the Commission established a framework for a voluntary cybersecurity labeling program for consumer wireless Internet of Things (IoT) products (IoT Labeling Program),[3] which includes selecting third party administrators to support the program.[4] The Commission delegated authority to the Bureau to open an initial filing window to receive applications from entities seeking

[1] While the Bureau may open additional filing windows at later dates, the Bureau will not accept applications for this initial round of applications that are filed after this filing window closes. However, applicants requiring additional time may, in accordance with Section 1.46 of the Commission's rules, request an extension of time for up to 10 additional calendar days to complete their applications. 47 CFR § 1.46.

[2] The Bureau sought comment on additional issues including withdrawal of CLA and Lead Administrator approval, recognition of CyberLABs located outside the U.S. by the Lead Administrator, complaints, and the registry, which will be addressed by the Bureau at a later date. Some of these issues will be part of the Lead Administrator's 90-day stakeholder engagement. The Bureau will rely, in part, on the notice and record developed in response to the June 2024 IoT Labeling Public Notice when considering the recommendations forthcoming from that stakeholder process supplemented, if warranted, based on subsequent recommendations or developments.

[3] *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*).

[4] *IoT Labeling Order* at 26, para. 48.

authority to be recognized as a CLA and those seeking to be recognized as the Lead Administrator.[5] CLAs will be authorized by the Commission to certify use of the FCC IoT Label, which includes the U.S. government certification mark (U.S. Cyber Trust Mark), by manufacturers whose products are found to be in compliance with the Commission's IoT cybersecurity labeling program rules.[6] The Lead Administrator will, among other duties, act as liaison between the Commission and CLAs, conduct stakeholder outreach to identify and/or develop and recommend to the Bureau technical standards and testing procedures for at least one class of IoT products, and in collaboration with CLAs, the FCC, and other stakeholders, develop and execute a plan for a consumer education campaign.[7]

II. CLA AND LEAD ADMINISTRATOR APPLICATIONS

A. Format of CLA and Lead Administrator Applications

3. In the *June 2024 IoT Labeling Public Notice*, the Bureau proposed that applications be submitted in narrative format via email and sought comment on this tentative determination.[8] We continue to believe that the information to be submitted by entities applying to be a CLA or Lead Administrator lends itself to a narrative discussion of their qualifications and adopt the narrative format proposed. While ioXt argues that a fillable form would better ensure uniformity among applications,[9] we believe the evaluation criteria and CLA/Lead Administrator responsibilities in the *IoT Labeling Order* are specific enough to allow for tailored applicant responses and comparative evaluation by the Commission at this time. In addition, as outlined by the Wi-Fi Alliance, "…a narrative format will better allow CLA applicants to describe in detail their expertise, the types of cybersecurity assessments in which they are involved, and how those activities and other qualifications will enable them to perform the CLA role. Because all these attributes are imperative to the performance of CLA responsibilities, a narrative will best allow the Commission to assess applicant qualifications."[10] UL Solutions also supports a narrative-format application, noting that this format will allow applicants to provide the detailed information needed to support their applications.[11] TÜV SÜD also commented that email is functional, and that a fillable form, while helpful for clarification, should also include a narrative text field so applicants can add relevant information.[12] One commenter, ioXt, expressed concern that a "narrative email" may require additional communication between staff and applicants to obtain all necessary information to evaluate an application.[13] We note that an enumeration of the evaluation criteria, and additional application instructions, including a "Frequently Asked Questions" link, are also provided below in this Public Notice

[5] *Id.* at 36, para. 64. The *IoT Labeling Order* also delegated authority to the Bureau to open additional filing windows or otherwise accept additional applications for authority to be recognized by the Bureau as a CLA when and as the Bureau determines it is necessary. *Id.*

[6] *Id*. at 26-27, para. 48.

[7] *Id*. at 27-29, para. 52.

[8] *Public Safety and Homeland Security Bureau Requests Comment on Implementation of the Cybersecurity Labeling for Internet of Things Program*, PS Docket No. 23-239, DA 24-617, at 2, para. 2 (June 27, 2024) (*June 2024 IoT Labeling Public Notice*).

[9] ioXt Comments at 1.

[10] Wi-Fi Alliance Comments at 2.

[11] UL Solutions Comments at 1 (UL Comments).

[12] TÜV SÜD Comments at 1.

[13] ioXt Comments at 1.

and will provide further guidance to applicants.[14] Further, the Bureau has considered and anticipates that staff may need to respond to applicant questions during the application review process and has designated staff for that purpose below.[15]

4. Entities applying to be a CLA or the Lead Administrator must file a narrative explanation of their qualifications to the Office of the Secretary.[16] Consistent with the record, we determine that CLA and Lead Administrator applications and supporting documentation shall be treated as presumptively confidential.[17] Each page of the application must be clearly and conspicuously labeled "**CONFIDENTIAL, NOT FOR PUBLIC INSPECTION**." As we expect applications will contain commercially sensitive and proprietary information that the Commission routinely treats as confidential, applications shall remain presumptively confidential, regardless of disposition of the application.[18] We decline to publish applications as a matter of course, including for those entities selected as CLAs or the Lead Administrator. We disagree with commenters who argue that the value of understanding CLA methodologies outweighs confidentiality protections,[19] as Commission evaluators will still have the opportunity to review the applicant's testing methodologies submitted to the agency. Maintaining the presumptive confidentiality of CLA and Lead Administrator applications, including those applications that are approved by the Bureau, will provide applicants with assurances that the commercially sensitive business information they submit in conjunction with their voluntary participation in the FCC's Program will not be publicly disclosed.[20] We believe maintaining the presumptive confidentiality of these applications will encourage additional entities to submit applications for these voluntary roles. Thus, in announcing the entities selected as CLAs and Lead Administrator, we only plan to make public the entity's name and their contact information.

5. While the Bureau will review the narrative applications received via email, we seek to leverage existing procedures, including records management, by building on a framework for the filing of confidential materials that the Commission has used in the past.[21] Consistent with that historical approach, applicants must file the application and supporting materials with the Office of the Secretary

[14] *Infra* Section IV.

[15] *Id*.

[16] As stated in the *2024 IoT Labeling Public Notice*, the Bureau may re-evaluate the need for a fillable form and seek additional comment on this issue after this CLA application filing window closes. *June 2024 IoT Labeling Public Notice* at 2, para. 2.

[17] While applicants may choose to file their application publicly, commenters broadly agreed that CLA and Lead Administrator applications presumptively should be treated as confidential at the pre-selection stage. *See, e.g.,* ITI Comments at 2; Logitech Comments at 1; NCTA Comments at 8-9; TÜV SÜD Comments at 4; UL Comments at 6; Letter from J. David Grossman, Vice President, Policy & Regulatory Affairs, CTA, Katie McAuliffe, Senior Director, Telecommunications Policy, Information Technology Industry Council, David Valdez, Vice President, Privacy and Cybersecurity, CTIA, Steve Griffith, Executive Director, Regulatory & Industry Affairs, National Electrical Manufacturers Association to Marlene H. Dortch, Secretary, FCC, PS Docket No. 23-239, at 3 (filed Sept. 10, 2024) (CTA et al. Letter).

[18] *See* ITI Comments at 2 (arguing applications should remain confidential at all stages to protect proprietary technology and trade secrets).

[19] Consumer Reports, Carnegie Mellon University, Public Knowledge, Electronic Privacy Information Center (EPIC), New York University Comments at 2 (CR et al., Joint Comments).

[20] As NCTA's comments recognize, to the extent that Commission records "would be subject to disclosure under the Freedom of Information Act," the Commission would have an obligation to make that available in accordance with that law and the Commission's implementing rules. NCTA Comments at 9. *See also, e.g.*, 47 CFR § 0.461.

[21] *See, e.g.*, *FCC Provides Further Instructions Regarding Submission of Confidential Materials*, Public Notice, DA 20-361 (Mar. 31, 2020).

either via hand or messenger delivery, by commercial overnight courier, or First-Class or overnight U.S. Postal Service mail. A copy must be sent to the Bureau via email as a password protected .pdf file to CyberTrustMark@fcc.gov. Additional instructions on submitting applications are provided below in Section IV.

B. FCC Filing Fees for CLA and Lead Administrator Applications

6. In the *June 2024 IoT Labeling Public Notice*, the Bureau sought comment on whether a filing with the Commission by an entity that is seeking to be a CLA or Lead Administrator constitutes an application under section 8 of the Communications Act, and if so, whether an existing FCC fee category would cover such applications or if a new application fee category should be established.[22] In addition, the Bureau sought comment on what fee the Commission should charge in connection with such a filing, if applicable.[23] Commenters do not opine on whether it is appropriate to charge application fees. The Association of Home Appliance Manufacturers (AHAM), however, explains that if fees are charged, they "should not be cost prohibitive to the point where it unnecessarily limits those entities that wish to apply."[24] TÜV SÜD does not comment on whether a fee should be assessed, but does indicate that if a fee is assessed, the Commission should set a new fee category.[25]

7. In this instance, our IoT Labeling Program derives in part from our authority to hold and utilize a registered certification mark.[26] In reviewing applications to be a CLA or Lead Administrator, we therefore are not acting solely under our Communications Act authority, but also to protect our registered certification mark. Given this dual role, at this time, we do not believe that the nature of our review of the

---

[22] The Commission has the authority to assess application fees under Section 8 of the Communications Act and has assessed application fees since 1986. Consolidated Omnibus Budget Reconciliation Act of 1985, Pub. L. No. 99-272, §§ 5002(e), (f), 100 Stat. 82, 118-121 (1986). In 2018, Congress revised the Commission's application fee authority by amending section 8 and adding section 9A to the Communications Act. Repack Airwaves Yielding Better Access for Users of Modern Services Act of 2018 (RAY BAUM'S Act), Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, 132 Stat. 1084, Division P, Title I, § 103 (2018). In order to implement the RAY BAUM'S Act, the Commission sought comment on and adopted a new streamlined schedule of application fees that aligns with the types of applications the Commission now receives and correlates the fees charged to the costs of processing the associated applications. *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, 1619, para. 3 (2020); *Application Fee NPRM*, 36 FCC Rcd at 1618-19, para. 1; *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); *See* 47 CFR subpart G (Schedule of Statutory Charges and Procedures for Payment).

[23] *See June 2024 IoT Labeling Public Notice* at 3-6, paras. 3-10.

[24] Association of Home Appliance Manufacturers Comments at 1 (AHAM Comments).

[25] TÜV SÜD Comments at 1.

[26] *See* 15 USC 1054 ("Subject to the provisions relating to the registration of trademarks, so far as they are applicable, collective and certification marks, including indications of regional origin, shall be registrable under this chapter, in the same manner and with the same effect as are trademarks, by persons, and nations, States, municipalities, and the like, exercising legitimate control over the use of the marks sought to be registered […].") and 15 USC 1127 ("In the construction of this chapter [the Lanham Act][…] [t]he term 'person' also includes the United States, any agency or instrumentality thereof, or any individual, firm, or corporation acting for the United States and with the authorization and consent of the United States. The United States, any agency or instrumentality thereof, and any individual, firm, or corporation acting for the United States and with the authorization and consent of the United States, shall be subject to the provisions of this chapter in the same manner and to the same extent as any nongovernmental entity.").

applications is such that they should be subject to an application fee.[27] We recognize that the process for applying to be a CLA or Lead Administrator may evolve with time. As such, we do not wholly foreclose adopting application fees in the future. Given these facts coupled with the lack of support in the record, the Bureau will not assess FCC application fees on CLA and Lead Administrator applications at this time.

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

8. The Bureau declines to expand the CLA and Lead Administrator selection criteria beyond what is set out in the *IoT Labeling Order*. In the *June 2024 IoT Public Notice*, the Bureau sought 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*. The Bureau also asked what additional criteria, if any, the Bureau should take into consideration during the Lead Administrator selection process, as well as safeguards the Bureau might adopt to ensure the stakeholder process remains competitively neutral and whether all selection criteria should be weighted the same.

9. NCTA suggests that "when selecting a Lead Administrator, the Bureau should consider candidates' ability to maintain the Program's integrity when translating the substantive technical security requirements into recommended standards and test procedures, and do so without creating unnecessary deterrents for manufacturer participation in the Program."[28] We agree that a Lead Administrator's maintenance of the Program's integrity during the 90-day stakeholder process and resulting recommendations is very important to the success of the Program. However, the Bureau finds that the criteria outlined in the *IoT Labeling Order* are sufficient to ensure the selected Lead Administrator has the technical experience and the high integrity expected of an entity supporting an FCC program. This position is supported by UL Solutions, which states the "[*IoT Labeling Order*] did not neglect any important considerations for assessing the qualifications of organizations to serve as CLAs or as the Lead Administrator."[29] We believe that the public/private partnership and close collaboration between industry and other stakeholders contemplated in *the IoT Labeling Order*, along with the Commission's oversight, will ensure that there are adequate guardrails to maintain the Program's integrity in this regard.[30]

10. NCTA also encourages the Bureau to evaluate Lead Administrator applications for their ability to avoid conflicts of interest, including any relationships the Lead Administrator applicant may have that could create the appearance of impropriety or a conflict of interest, such as complaints from manufacturers, and suggests evaluating whether Lead Administrator applicants have the financial resources to avoid such conflicts going forward.[31] We disagree that it is necessary to take additional measures when evaluating applications for this purpose. Existing application criteria require an applicant to describe their organization structure, including an explanation of how it will avoid personal and

---

[27] The decision in section II.B of this Public Notice is made in conjunction with the Office of Managing Director (OMD). *See IoT Labeling Order* at 36, para. 64 (delegating "to PSHSB and OMD authority to take any necessary steps, including adoption of additional procedures and any applicable fees after selection of the CLAs, if necessary to ensure compliance with the Communications Act or applicable government-wide statutes that are implicated by the IoT Labeling Program").

[28] NCTA Comments at 4.

[29] UL Comments at 2.

[30] *IoT Labeling Order* at 2, para. 2 ("[r]ecognizing that a successful voluntary IoT Labeling Program will require close partnership and collaboration between industry, the federal government, and other stakeholders" and adopting "an administrative framework for the IoT Labeling Program that capitalizes on the existing public, private, and academic sector work in this space, while ensuring the integrity of the IoT Labeling Program through oversight by the Commission.").

[31] NCTA Comments at 7.

organizational conflict when processing applications, and demonstrate implementation of controls to eliminate actual or potential conflicts of interests (both personal and organizational), to remain impartial and unbiased.[32] In addition, the Future of Privacy Forum urges the Bureau to "consider requiring program administrators to possess relevant privacy expertise as well as cybersecurity expertise."[33] We agree that privacy is an integral aspect of cybersecurity, and note that existing application criteria require applicants to possess both privacy and cybersecurity expertise, including demonstrated expert knowledge of the National Institute of Standards and Technology (NIST) cybersecurity guidance and recommended criteria and labeling program approaches, which include privacy among their core cybersecurity capabilities.[34]

11. We also note that the Wi-Fi Alliance recommends that in addition to demonstrating their "[e]xpert knowledge of FCC rules and procedures associated with product compliance testing and certification," CLA applicants also demonstrate their *experience* in this area.[35] Wi-Fi Alliance recognizes that while a lack of current experience with developing and implementing security standards should not be disqualifying, it would serve the public interest for the Bureau to include this "additional requirement, particularly concerning specific IoT products where cybersecurity standards have already been developed and tested."[36] The Wi-Fi Alliance encourages the Bureau to give a preference to CLA applicants with this experience.[37] The Bureau declines to require applicants to demonstrate previous experience with FCC rules and procedures associated with product compliance testing and certification as a condition precedent to being an approved CLA or give preference to CLA applicants with this experience. In particular, applicants are always encouraged to provide any additional information that helps demonstrate their expertise or experience under the relevant criteria and, providing examples of an applicant's experience where applicable, in general, will provide more information from which the Bureau can evaluate an application.[38] Additionally, CTIA proposes criteria for evaluating CLA applications to include a minimum of 5-10 years of experience managing a cyber certification program and proven experience in running or participating in a working group on cybersecurity standards.[39] While we agree that this set of criteria can be useful to demonstrate a "proven track record," we are concerned that requiring such specific criteria may unnecessarily exclude applicants that otherwise may have appropriate knowledge and expertise. Therefore, we decline to adopt this recommendation.

12. We conclude that we will maintain the criteria as set out in the *IoT Labeling Order* for the initial round of CLA and Lead Administrator applications. The Bureau, jointly with OMD and, to the extent necessary, Office of General Counsel, will receive and review administrators' applications for compliance with each criteria set forth in the *IoT Labeling Order* and to best ensure the success of the

---

[32] *See IoT Labeling Order* at 32-33, para. 59.

[33] Future of Privacy Forum Comments at 4.

[34] *IoT Labeling Order* at 32-33, para 59. *See also*, NIST, NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline* (2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf.

[35] Wi-Fi Alliance Comments at 3.

[36] *Id.*

[37] *Id.*

[38] *See infra* note 125 (providing that Applicants may, for example, demonstrate experience with the FCC's Equipment Authorization Program or another FCC-run compliance program with respect to FCC rules and procedures associated with product compliance testing and certification).

[39] CTIA Comments at 14.

program.[40] We note that UL Solutions recommends certain requirements be defined in greater detail to avoid subjective determinations,[41] but we believe that the *IoT Labeling Order* provided a comprehensive list of required criteria that covers the breadth of expertise and capabilities necessary to select a CLA and Lead Administrator at this early stage of the program and is neutral toward applicants.[42] Further, as noted above, applicants are not limited to providing the required criteria listed in the *IoT Labeling Order*, but have the flexibility to offer additional expertise or selection criteria they believe are pertinent and support their application (e.g., expected costs/budget for Lead Administrator to carry out their responsibilities, information to support their ability to carry out the respective responsibilities, etc.). Should the Bureau conclude that it would be appropriate to open subsequent filing windows, we may seek comment on, and consider adoption of, additional selection criteria at that time.

13. As discussed in the *IoT Labeling Order*, authorizing one or more CLAs subject to Commission oversight to handle the routine administration of the program will help to ensure its timely and consistent rollout, and independent third-party CLAs will bring trust, consistency, and an impartial level playing field to the IoT Labeling Program and will provide the required expertise for the administration of the program. Leveraging the expertise of multiple existing program managers and using pre-existing systems and processes that meet our program specifications will minimize administrative delay and ensure the Commission effectively utilizes the expertise of those entities who have made investments in their own cybersecurity labeling programs. Entities that have experience working with manufacturers and IoT conformity and standards testing, as required in the criteria adopted in the *IoT Labeling Order*, will also best be able to promote an efficient and timely rollout of the IoT Labeling Program.

14. We disagree with CTIA's suggestion that the Bureau adopt a flexible approach with respect to International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17065 accreditation requirements for CLAs with a certain level of experience to avoid unnecessary costs and delays.[43] CTIA posits that "[accreditation] can be costly and time-consuming to obtain and is unnecessary for prospective CLAs that have demonstrated track records in managing similar certification programs."[44] Instead, CTIA proposes for entities with at least 5-10 years of experience running certification programs, ISO/IEC 17065 accreditation should be optional.[45] In contrast, A2LA submits that the "ISO/IEC 17065 accreditation requirement will be of benefit to the FCC and the consumers it serves by providing necessary risk mitigation… Claiming a certain number of years' experience is not equivalent to demonstrating technical competence or compliance."[46] The *IoT Labeling Order* and accompanying rules require that all CLAs obtain ISO/IEC 17065 accreditation to the Commission's scope within six months of the effective date of the adopted standards and testing

---

[40] IoT Labeling Order at 36, para 64; *see also* ioXt Comments at 4 (recommending that all selection criteria be weighted the same).

[41] UL Comments at 3.

[42] *See also* AHAM Comments at 1-2 (suggesting that the selection criteria should be neutral toward applicants and that applicants should have the necessary expertise to serve in these functions).

[43] CTIA Comments at 14.

[44] CTIA argues that "[w]hile ISO/IEC accreditation can be a helpful metric for organizations with limited practical experience, it can be costly and time-consuming to obtain and is unnecessary for prospective CLAs that have demonstrated track records in managing similar certification programs." CTIA Comments at 14.

[45] CTIA Comments at 14. *See also* CTIA Reply Comments at 2 ("the FCC should not require ISO/IEC accreditation for those CLA applicants that have significant experience functioning in a similar role.")

[46] A2LA Reply Comments at 1.

procedures.[47] The Commission previously determined that "leveraging accredited industry bodies to perform conformity assessments will 'speed the establishment of the program and increase the program's ultimate quality.'"[48] As such, we decline to adopt CTIA's suggested exemption. Alternatively, CTIA recommends an 18-month grace period to obtain such accreditation, for entities that have a proven track record of successfully managing a certification program.[49] The Commission recognized it would take time for selected CLAs to obtain ISO/IEC 17065 accreditation and for that reason found it appropriate to conditionally approve CLAs and allow an additional six months for selected administrators to obtain accreditation.[50] While we decline to adopt a blanket 18-month grace period, we are mindful that some entities may require more than six months to obtain accreditation. We think the Commission's existing rule waiver procedure[51] is an appropriate and sufficient vehicle for CLAs that cannot meet the accreditation deadline to request a waiver of the rule along with their requested extension period.

15. We also disagree with CTA's suggestion that conditional approval of CLA applications will allow CLAs to certify products to use the FCC IoT Label before obtaining ISO/IEC 17065 accreditation to the Commission's scope.[52] The Commission indicated that CLA applications will be conditionally approved in order to expedite initial deployment of the FCC's program.[53] However, CLAs that have not demonstrated that they have received ISO/IEC 17065 accreditation to the Commission's scope will not be recognized and approved by the Bureau to receive applications or otherwise approved to authorize use the FCC IoT Label.[54]

16. It is premature for the Bureau to address the specific scope of the Commission's accreditation program as the standards and testing procedures have not yet been adopted. However, we emphasize that each CLA will be required to obtain ISO/IEC 17065 accreditation to the FCC scope before it will be recognized by the Commission as an entity authorized to certify a product as being compliant with FCC IoT Labeling Program rules and authorize use of the FCC IoT Label consistent with the *IoT Labeling Order*.[55]

D. Lead Administrator Expenses Shared Among CLAs

---

[47] *IoT Labeling Order* at 32-33, para. 59(6); 47 CFR § 8.220(c)(6).

[48] *IoT Labeling Order* at 38, para 68 (citing CTA Oct. 6, 2023 Comments at 18).

[49] CTIA Comments at 15 and CTIA Reply Comments at 2.

[50] *IoT Labeling Order* at 32-33, para 59(6).

[51] 47 CFR § 1.925.

[52] CTA Comments at 13. CTA also recommends the Bureau similarly conditionally approve CyberLABs to begin testing products before they become accredited and provide CyberLABs a 6-month grace period to obtain accreditation, which the Bureau declines to do. Letter from J. David Grossman, Vice President, Policy & Regulatory Affairs, CTA, and Mike Bergman, Vice President, Technology & Standards, CTA, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 23-239, at 2 (filed Aug. 14, 2024) (CTA *Ex Parte*). CyberLABs are not authorized by the Commission to begin testing products for compliance with the IoT Labeling Program until after they have obtained the appropriate accreditation to the Commission's scope and have been recognized by the Lead Administrator. *See* 47 CFR § 8.218.

[53] 47 CFR § 8.220(c)(6).

[54] *IoT Labeling Order* at 32-33, para 59(6).

[55] *Id.* at 32-33, para. 59(6); 47 CFR § 8.220(c)(6).

17. The *June 2024 IoT Labeling Public Notice* sought recommendations for an effective mechanism for CLAs to share the Lead Administrator's expenses.[56] Parties are generally in agreement that Lead Administrator startup costs will be higher than the Lead Administrator's ongoing costs once the program is stood up and should be reflected in the CLA's cost sharing obligations.[57] UL Solutions recommends an initial standup fee for the Lead Administrator and a per-certificate fee going forward.[58] The Wi-Fi Alliance recommends the Lead Administrator submit to the Bureau a claim for expenses incurred in the performance of its duties, which if approved, would be shared proportionally among the CLAs, with the proportionality being based on the annual number of products the CLA certifies to use the FCC IoT Label.[59] The Wi-Fi Alliance notes that Lead Administrator expenses subject to sharing by the CLAs should be limited to those "that are unique to the Lead Administrator *as Lead Administrator*,"[60] and not related to its activities as a CLA.

18. The Bureau recognizes that the Lead Administrator's expenses incurred as a result of the performance of its duties under this program must be reasonable and accurately reflect its actual costs. In addition, it is also important to ensure each CLA shares in the Lead Administrator's costs as required by the *IoT Labeling Order*[61] and that the costs shared reflect the Lead Administrator's actual and reasonable expenses incurred as a result of performance of its Lead Administrator duties and only those expenses incurred in its capacity as Lead Administrator. To ensure this occurs, the Lead Administrator is required to implement internal controls adequate to ensure its operations maintain best practices to protect against improper payments and to prevent fraud, waste, and abuse in its handling of funds. Once selected, the Lead Administrator will also submit to the Bureau and OMD, an estimate of its forward-looking costs including, separately, program stand-up costs and ongoing program costs to perform the Lead Administrator duties for the Lead Administrator's upcoming calendar year, which will be reviewed by CLAs, PSHSB, and OMD for reasonableness, and if determined to be reasonable by PSHSB and OMD, will be used to estimate the overall CLA cost sharing obligation.[62]

19. Consistent with the *IoT Labeling Order*, each CLA will share in these Lead Administrator costs, however, we decline to establish the methodology for such cost sharing and instead

---

[56] *June 2024 IoT Labeling Public Notice* at 6, para. 12.

[57] *See* ioXt Comments at 4 (fees may be higher during the initial rollout of the program, but should be lowered in the following year(s) as there will not be a need for as much 'set up' costs."); UL Comments at 2.

[58] UL Comments at 2.

[59] Wi-Fi Alliance Comments at 4-5. The Wi-Fi Alliance notes the Commission has adopted a similar process requiring the Commission review costs as reasonable in other FCC-run programs, including the Commission's Universal Service Rules, (47 CFR §§ 54.701-54.717, 54.719-54.725) where the Commission reviews and approves projected quarterly budgets before the Universal Service Administrative Company (USAC) disburses funds and the white space rules (47 CFR §54.715), where the white space database administrator collects fees for its services as administrator, but the Commission "upon request will review the fees and can require changes in those fees if they are found to be excessive.'" Wi-Fi Alliance Comments at 5. The Wi-Fi Alliance also points to the Commission's Citizen Broadband Radio Service (CBRS) rules (47 C.F.R. § 96.65) where the Spectrum Access System administrators charge CBRS users a "reasonable fee" that is subject to review by the Commission. Wi-Fi Alliance Comments at 5.

[60] Wi-Fi Alliance Comments at 5-6.

[61] *IoT Labeling Order* at 47, para. 93.

[62] CTIA, and others, point out the need for federal funding to support core aspects of the program, such as consumer education. CTIA Comments at 3; CTIA Reply Comments at 3; CTA Comments at 15; NCTA Comments at 10. NCTA argues the Federal government should lead the consumer education campaign, which would reduce the burden on the Lead Administrator and CLAs. NCTA Comments at 5. However, both of these recommendations are beyond the Bureau's delegation of authority and the scope of this Public Notice.

rely on CLAs and the Lead Administrator to determine the sharing methodology, which should be reasonable and equitable and will be subject to ongoing oversight by the Commission.[63] Further, we require the Lead Administrator to submit to the Bureau and OMD, an annual, independently audited, statement of program expenditures and monies received from the CLAs due before the end of the calendar year.[64] The Bureau will provide further guidance on CLA cost sharing once the CLAs and the Lead Administrator have been selected.[65]

E. Lead Administrator Neutrality

20. *Neutral Treatment of CLAs and Other Stakeholders.* In the *IoT Labeling Order*, the Commission recognized the competitive implications of an entity being both the Lead Administrator and a CLA.[66] The *June 2024 IoT Labeling Public Notice* sought comment on what safeguards, if any, the Bureau should adopt to ensure Lead Administrator neutrality as a potential competitor of other CLAs.[67] The Bureau also asked whether there are additional safeguards, beyond those contemplated in the *IoT Labeling Order*,[68] the Bureau should adopt to ensure the stakeholder engagement process and related recommendations the Lead Administrator makes to the Commission (*e.g.*, standards and testing criteria and label design) are consensus-based and competitively neutral.[69]

21. Commenters emphasize the importance of ensuring Lead Administrator neutrality to prevent actual, as well as perceptions of, unfair economic advantage by the Lead Administrator over other CLAs,[70] and support adopting reasonable safeguards to do so.[71] We share ioXt's concern that if the Lead Administrator gained an economic advantage by passing on fees to other CLAs, for example, CLAs would have to raise their prices, which would pass on the costs to the manufacturers, and then on to consumers.[72] In order to ensure impartiality, A2LA recommends considering ISO/IEC 17065 requirements, which describe a mechanism (often a committee) for safeguarding impartiality and assuring a competitively neutral environment between the Lead Administrator, CLAs, and other stakeholders.[73] TÜV SÜD also recommends that Lead Administrator neutrality be evaluated on a yearly basis, with the

---

[63] *See, e.g.*, ioXt Comments at 4 ("There should be a neutral oversight committee, such as The Bureau, who would review the expenses a Lead Admin would incur and guide a decision towards and appropriate amount to charge CLAs."); *see also* NCTA Comments at 5 (stating "the expense sharing mechanism [should] enable[] the Lead Administrator to recoup its costs and effectively support the Program's needs for maximum consumer benefit, while maintaining economic incentives for CLA and manufacturer participation").

[64] The Commission "delegated authority to the Bureau to release a Public Notice announcing the CLA(s) selected by the Bureau and next steps for each entity, including but not limited the execution of appropriate documentation governing the details of the CLA's responsibilities." *IoT Labeling Order* at 36, para 64.

[65] We thus leave pending the notice provided in this regard in the *June 2024 IoT Labeling Public Notice*.

[66] *See IoT Labeling Order* at 32, 36, paras. 59, 64 & n.237.

[67] *June 2024 IoT Labeling Public Notice* at 7, para. 13.

[68] *See* 47 CFR § 8.220(c)(8).

[69] *Id.*

[70] *See* TIC Council Americas Comments at 2 (TIC Comments); NCTA Comments at 6; Wi-Fi Alliance Comments at 6; ioXt Comments at 5; UL Comments at 4; Infineon Technologies Americas, Corp. Comments at 3 (Infineon Comments).

[71] *See* AHAM Comments at 1-2, Somos, Inc. Comments at 5 (Somos Comments).

[72] ioXt Comments at 5.

[73] A2LA Comments at 2.

possibility of triggering an investigation by the Commission and revocation of Lead Administrator designation.[74] Infineon suggests requiring a "firewall" to separate the Lead Administrator from its role as CLA, similar to those instituted by law firms to avoid conflicts between multiple clients' interests.[75] Somos, Inc. recommends applying relevant rules from its role as the North American Numbering Plan Administrator to the Lead Administrator, including impartial allocation of resources, transparency, non-discrimination, avoidance of conflicts of interest, and compliance with regulations.[76]

22. We agree that ensuring Lead Administrator neutrality "is critical to maximizing the Program's credibility and fostering trust among stakeholders,"[77] and we believe the *IoT Labeling Order* sufficiently addresses the concerns raised in the record. We note that the requirement that the Lead Administrator be accredited to ISO/IEC 17065 will ensure that the entity is appropriately aligned with those impartiality mechanisms. Further, we require all CLA applicants, including those applying to be the Lead Administrator, to demonstrate implementation of controls to eliminate actual or potential conflicts of interests, including remaining impartial and unbiased.[78] The Bureau will evaluate such applications to ensure rigorous compliance with this criteria. We also note that approval of the Lead Administrator may be subject to withdrawal by the Commission upon a determination of just cause,[79] and this includes failing to follow those impartiality requirements. The Lead Administrator must be committed to neutrality and impartiality, consistent with the *IoT Labeling Order*.[80] Because we anticipate those measures will be sufficient, we are not persuaded of the need to adopt additional requirements at this time.

23. Finally, CTA proposes asking prospective CyberLABs and CLAs to attest that they meet the requirements in the (draft) CTA-2119 Scheme Assessment Framework, as an industry consensus standard to preserve neutrality when assessing applicant entities.[81] We decline to adopt this requirement at this time, given that the draft CTA-2119 Framework has not undergone public notice and comment.[82] However, we may reconsider this proposal at a later date, once the Labeling Program's standards and testing procedures have been finalized.[83]

24. *Transparency in 90-day Stakeholder Process*. As an initial matter, we emphasize that the *IoT Labeling Order* requires the Lead Administrator to "provide equitable recommendations to the Commission to encourage the broadest possible participation of CLAs within the parameters of the FCC's rules."[84] Therefore, while we believe it is premature to adopt additional rules in this regard, we note that UL Solutions emphasizes the importance of transparency in the stakeholder collaboration process, stating that the Lead Administrator should invite a wide variety of stakeholders and ensure they all have

---

[74] TÜV SÜD Comments at 2-3.

[75] Infineon Comments at 3.

[76] Somos Comments at 3-4.

[77] NCTA Comments at 6.

[78] *See IoT Labeling Order* at 33, para. 59(7).

[79] *See* 47 CFR 8.220(e)(2)-(e)(5).

[80] *IoT Labeling Order* at 33, para. 59(7).

[81] CTA Comments at 13-14.

[82] *See* 5 U.S.C. § 553.

[83] CTA also proposes applying the CTA-2119 Scheme Assessment Framework as a uniform way to evaluate whether a scheme recommended by the Lead Administrator-led working group meets the NISTIR 8425 criteria required in the *IoT Labeling Order*. CTA Comments at 13. We similarly decline to adopt this proposal at this time.

[84] *IoT Labeling Order* at 36, para. 64.

sufficient opportunity to have their views heard and participate in manageable working groups.[85] Further, UL Solutions states that recommendations made to the Commission should also include dissenting views and how those dissenting views were addressed, which would be considered in the final rules adopted by the Commission.[86] UL Solutions also recommends the importance of a clear and transparent process to shield the Lead Administrator from accusations or perceptions of bias when recognizing accredited CyberLABs.[87] TÜV SÜD similarly proposes safeguards, such as a mandatory consultation round before making critical decisions regarding recommendations to the Commission.[88]

25. While we do not adopt additional guardrails at this stage, we reiterate the position in the *IoT Labeling Order* that the Lead Administrator should ensure participation from a wide variety of stakeholders and consider various resources when developing the IoT Labeling Program recommendations.[89] As noted above, ISO/IEC 17065 accreditation is required for all CLAs, including the Lead Administrator, and adherence to that standard requires the convener of working groups to develop recommendations (here, the Lead Administrator), and achieve a balanced representation of interests, such that no single interest predominates.[90] We agree that transparency in the 90-day stakeholder process is of the highest importance and the Bureau expects to provide additional guidelines on that process when it announces the selection of CLAs and the Lead Administrator.[91]

F. Confidentiality and Security Requirements

26. The Bureau adopts its proposal from the *June 2024 IoT Labeling Public Notice* that manufacturer applications submitted to CLAs are presumptively confidential and CLAs are required to maintain this confidentiality.[92] CLAs will be required to maintain the confidentiality of non-public information received as part of an application for authority to use the FCC IoT Label, and must implement appropriate administrative, technical, procedural, and physical safeguards to protect the confidentiality of information received by the CLA and protect against the unauthorized disclosure and unauthorized use of non-public information received as a result of its participation in the FCC IoT Labeling Program.

27. We agree with commenters that the program would benefit from a presumption of confidentiality for filings and related information provided to CLAs from applicants seeking use of the FCC IoT Label, which would encourage manufacturer participation and protect proprietary technology and trade secrets.[93] We disagree with commenters that such a presumption of confidentiality is not

---

[85] UL Comments at 4.

[86] *Id.* at 4.

[87] *Id.* at 3.

[88] TÜV SÜD Comments at 2.

[89] *See IoT Labeling Order.* at 30-32, paras. 56-58. *See also* Wi-Fi Alliance Comments at 6 (agreeing that Lead Administrator neutrality should be ensured through disclosures of any associations that may materially impact their impartial administration and that their recommendations should be subject to review by the Bureau).

[90] *See id.*; ISO/IEC 17065, 5.2.2–5.2.4.

[91] We thus leave pending the notice provided in this regard in the *June 2024 IoT Labeling Public Notice*.

[92] *June 2024 IoT Labeling Public Notice* at 9, para. 17. *See also* CTA et al. Letter at 3 (recommending the Bureau treat manufacturer applications as presumptively confidential).

[93] *See* ITI Comments at 2; Logitech Comments at 1; NCTA Comments at 8; CTA Comments at 14. *See also* A2LA Comments at 3 (stating that conformity assessment bodies participating in the program should adhere to confidentiality requirements defined in ISO/IEC 17065).

necessary due to the public-facing nature of the label.[94] While this is true for product information required to be disclosed in the registry if approval is granted,[95] this would not be the case for products that are denied authorization to bear the FCC IoT Label. In addition, as discussed above, we expect that applications submitted to the Commission by CLAs will also continue to be treated as presumptively confidential.[96] We emphasize here that information submitted by manufacturers to CLAs, the Lead Administrator, and/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.

28. In the *June 2024 IoT Labeling Public Notice*, the Bureau tentatively concluded that the requirements of the Federal Information Security Modernization Act of 2014 (FISMA)[97] apply to the Lead Administrator and CLAs.[98] Some commenters oppose a FISMA requirement, stating that it would "strongly discourage CLAs from applying to the program,"[99] and that FISMA has not been applied by other agencies supporting analogous programs, such as the Health and Human Services Department's Office of the National Coordinator's (ONC) certification program for health IT products.[100] While we acknowledge these concerns, alone, they are not dispositive for not applying FISMA.

29. FISMA was enacted to ensure that each federal agency develops, documents, and implements an agency-wide program to secure federal information systems[101] from unauthorized access, use, disclosure, disruption, modification, or destruction.[102] Given this scope, we reconsider our tentative conclusion to apply FISMA to CLAs and the Lead Administrator and determine that, as presently contemplated, neither the CLAs nor the Lead Administrator will operate an information system on behalf of the agency. That is so because the Commission has no plans to establish any interconnection between

---

[94] CR et al., Joint Comments.

[95] *See* UL Comments at 6.

[96] *See* A2LA Comments at 3; Logitech Comments at 1.

[97] *Federal Information Security Management Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899 (2002); amended by *Federal Information Security Modernization Act of 2014* (FISMA), Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014).

[98] *June 2024 IoT Labeling Public Notice* at 9, para. 19. The *June 2024 IoT Labeling Public Notice* also asks whether "…the registry operator(s) [should] as appropriate, be required to implement adequate security, privacy, and availability controls to meet FISMA low/moderate standards, or a commercial equivalent?" *Id*. at 12, para 24. The Bureau recognizes the importance of the registry's security requirements, and will address these issues in a future Public Notice addressing the structure of the Registry's Application Programming Interface (API).

[99] ioXt Comments at 8. *See also* TIC Comments at 3-4 ("The additional burden of FISMA requirements will almost certainly reduce the willingness of potential applicants to participate in the program.").

[100] UL Comments at 6.

[101] FISMA defines a "Federal Information System" as "an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency." 40 U.S.C. § 11331(g)(2).

[102] *See* NIST, Computer Security Resource Center, *NIST Risk Management Framework*, *Federal Information Security Modernization Act (FISMA) Background*, https://csrc.nist.gov/projects/risk-management/fisma-background, (last accessed Aug. 22, 2024). *See also* 44 U.S.C. § 3552(b)(3) (stating "the term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction").

its systems and the Lead Administrator's or CLA's information systems; indeed, the FCC does not expect to routinely request, obtain access to, otherwise collect, use, process, or maintain the data or information held by the Lead Administrator or the CLAs, excepting for investigative purposes. Moreover, although the Lead Administrator will receive information from CLAs and applicant manufacturers necessary for it to carry out its responsibilities under the FCC's program, and CLAs will receive and evaluate applications and supporting data from applicant manufacturers, this, without more, does not mean that the Lead Administrator or CLAs are managing their information systems "on behalf of" the FCC.

30. Nevertheless, we agree with NCTA that "[c]lear guidelines, safeguards, and protocols for handling confidential information should be established to prevent unauthorized disclosure"[103] and believe that other mature security frameworks may be applied to CLAs and the Lead Administrator to reduce the risk of unauthorized access, use, disclosure, disruption, modification, or destruction of program data. Accordingly, we require that all CLAs and the Lead Administrator create, update, and implement cybersecurity risk management plans. Such a cybersecurity risk management plan must identify the cyber risks that the entity faces, the controls used to mitigate those risks, and the steps taken to ensure that these controls are applied effectively to their operations. The plans must also describe how each entity employs its organizational resources and processes to ensure the confidentiality, integrity, and availability of its information and information systems. These requirements are consistent with the National Cyber Strategy and are in keeping with a whole-of-government effort to "establish cybersecurity requirements to support national security and public safety."[104] We expect that creating, updating, and implementing a cybersecurity risk management plan will help protect each CLA and the Lead Administrator from serious national security threats.

31. We note that, under this approach, each entity has flexibility to structure its cybersecurity risk management plan in a manner that is tailored to its operations after consideration of a variety of factors, provided that the plan demonstrates that the entity is taking affirmative steps to analyze security risks and improve its security posture. We further note that an entity could successfully demonstrate satisfaction with this requirement by following an established risk management framework, such as the NIST Cybersecurity Framework (CSF)[105] or Risk Management Framework (RMF).[106] CLAs and the Lead Administrator security plans should be informed by established cybersecurity best practices such as the standards and controls set forth in the Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Cross-sector Performance Goals and Objectives (CISA CPGs),[107] ISO/IEC 27001,[108] NIST Special Publication 800-53 (rev 5),[109] or the Center for Internet Security Critical Security Controls (CIS

[103] NCTA Comments at 8.

[104] White House, National Cyber Strategy at 8 (2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[105] *See* NIST, The NIST Cybersecurity Framework (CSF) 2.0 (2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[106] *See* NIST, *Risk Management Framework for Information Systems and Organizations*, Special Publication 800-37 (rev. 2 2018), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[107] *See* Cybersecurity and Infrastructure Security Agency, Cross-Sector Cybersecurity Performance Goals and Objectives, https://www.cisa.gov/cpgs (last visited Mar. 15, 2024).

[108] *See* ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, https://www.iso.org/standard/27001.

[109] NIST, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53 (rev. 5 2020); *see also* NIST *Control Baselines for Information Systems and Organizations*, SP-800-53B (2020).

Controls) version 7.1 or later.[110] These frameworks are designed to be scalable and adaptable to the needs and capabilities of companies both large and small, are well understood by industry, and are flexible. CTIA and CTA argue compliance with a commercial equivalent framework to FISMA, such as ISO 27001 can "take a year or more at a cost upwards of $100,000."[111] However, these cost and timelines would not apply to this program, because while we require entities to implement security plans reflecting standards and controls, such as ISO/IEC 27001, we do not specifically require a CLA or the Lead Administrator to be certified to ISO/IEC 27001. Moreover, we expect that many entities in the industry that might seek to be CLAs or the Lead Administrator will have adopted plans along the lines we require here and may have obtained such certifications in the ordinary course of business. And in any event, we find that any costs that might be incurred by an entity seeking to be a CLA or Lead Administrator are outweighed by the benefits that will redound to such entities themselves, the industry more broadly, and U.S. national security from our requiring such entities to take these steps to protect the confidentiality, integrity, and availability of the information they hold—including from other entities in the industry—and the information systems they maintain. We expect risk management plans to contribute to the CLAs' and the Lead Administrator's existing internal security practices that maintain the confidentiality, integrity, availability of all information received in support of this program without significantly increasing the time or costs of participation.[112]

32. We additionally require each applicant seeking to serve as a CLA or Lead Administrator to submit with its application an attestation that it already has created and implemented - or upon selection will create and implement - a cybersecurity risk management plan as described above - which will demonstrate compliance with these requirements as well as the entity's cybersecurity expertise and capabilities, knowledge of NIST's cybersecurity guidance, and knowledge of federal law and guidance governing the security and privacy of information systems.[113] We also require that CLAs and the Lead Administrator make such cybersecurity risk management plans available to the Commission upon request. Access to cybersecurity risk management plans will allow the Commission to confirm whether plans are being regularly updated, to review a specific plan as needed, or to proactively review a sample of plans to confirm they sufficiently identify the cybersecurity risks to the Lead Administrator and CLAs in this program. In such circumstances, cybersecurity risk management plans would be presumptively confidential.

[110] *See* Center for Internet Security, Critical Security Controls Version 8, https://www.cisecurity.org/controls (last visited Mar. 15, 2024) (providing security controls grouped by priority and feasibility for different sizes and resources of businesses in Implementation Groups).

[111] CTIA Reply Comments at 9; CTA Comments at 10.

[112] We expect CLA and Lead Administrator applicants to address these internal security practices in their applications to the Commission, which will be enforceable under the Commission's rules. *See infra* para. 37.a. ("Applicant certifies that all statements made in this application and in the exhibits, attachments, or documents incorporated by reference are material, are part of this application, and are true, complete, correct, and made in good faith, *see* 47 CFR §§ 1.17, 8.220, 8.221.").

[113] *See infra* Section IV.

III. WHO MAY APPLY

33. Any domestic, independent,[114] non-governmental entity eligible to enter into a licensing agreement with the FCC may apply for the role of CLA and/or Lead Administrator;[115] however, an applicant cannot be owned or controlled by, or affiliated with, any entity that produces equipment on the FCC Covered List or is otherwise prohibited from participating in the IoT Labeling Program, to include companies named on the Department of Commerce's Entity List and the Department of Defense's List of Chinese Military Companies.[116]

IV. APPLICATION PROCEDURES

A. Applications for Cybersecurity Label Administrator (CLA)

34. Applicants seeking the role of CLA must demonstrate the following:

a. Applicant is not owned or controlled by or affiliated[117] with any entity identified on the Commission's Covered List, or is otherwise prohibited from participating in the IoT Labeling Program,[118] including being an entity identified on the Department of Commerce's Entity List[119] or on the Department of Defense's List of Chinese Military Companies;[120]

b. 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

---

[114] Here, "independent" means the applicant is not affiliated with or a subsidiary of another CLA/Lead Administrator applicant. *See IoT Labeling Order* at 32, 36, paras. 59, 64 & n.237. It also means that the applicant is a disinterested third-party outside of a prospective manufacturer's control that is applying for authority to use the FCC IoT Label. *See IoT Labeling Order* at 45, para. 87.

[115] The *IoT Labeling Order* declined to require that a CLA be a non-profit, stating that a for-profit or non-profit organization could possess the requisite qualifications and carry out the CLA duties effectively. *See IoT Labeling Order* at 35, para. 62. We note that Congress, from time to time, adopts appropriation riders that preclude federal agencies from entering into agreements with certain entities. *See e.g.* Section 744 and 745 of Title VII, Division B, of Further Consolidated Appropriations Act, 2024 –Pub. L. No. 118-47 (3/23/24) (precluding entering into agreements with corporations with certain felony convictions or unpaid Federal tax liability).

[116] *Id.* at 33, para 59(8).

[117] 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. The term *own* means to own an equity interest (or the equivalent thereof) of more than 10 percent. *See* 47 C.F.R. § 8.203(a); 47 U.S.C. § 153(2). *See also IoT Labeling Order* at 33, para. 59.

[118] *See IoT Labeling Order* at 33, 40, paras. 59, 74. The *Order* includes this catchall for entities otherwise prohibited from participating in the program, to include those listed in 47 CFR § 8.204 and those considered a "foreign adversary" country as defined by the Department of Commerce. *See id. See also id.* at 34-35, para. 61; 15 CFR § 7.4.

[119] *See* Bureau of Industry and Security, U.S. Department of Commerce, Supplement No. 4 to Part 744 – Entity List (2023), https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file.

[120] *See* Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. ("Mac") Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283), Tranche 2, U.S. Department of Defense (2022), https://media.defense.gov/2022/Oct/05/2003091659/-1/-1/0/1260H%20COMPANIES.PDF.

awards, to include all entities and individuals published as ineligible for award on the General Service Administration's System for Award Management;[121]

c. Description of Applicant's organization structure;[122]

d. Implementation of controls 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 Applicant from giving preferential treatment to certain applications particularly with regard to applicants from entities with whom the CLA has a business relationship (e.g., application line jumping or same level of scrutiny when reviewing the application) and from implementing heightened scrutiny of applications from entities not members or otherwise aligned with the CLA;[123]

e. Description of the process(es) Applicant will use to evaluate applications seeking authority to use the FCC IoT Label;[124]

f. Cybersecurity expertise and capabilities, in addition to industry knowledge of IoT generally, and IoT Labeling requirements;

g. 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;

h. Expert knowledge of FCC rules and procedures associated with product compliance testing and certification;[125]

i. Knowledge of Federal law and guidance governing the security and privacy of agency information systems; and[126]

j. The ability to securely handle large volumes of information, including a description of Applicant's related internal security practices.

35. Applicants seeking the role of CLA must also commit to complying with the obligations of CLAs under the *IoT Labeling Order* and the Commission's rules, including but not limited to the

---

[121] *See* U.S. General Services Administration System for Award Management, *Exclusion Types*, https://sam.gov/content/entity-information/resources/exclusion-types (last visited Feb. 15, 2024).

[122] In describing its organizational structure, an Applicant may describe its relevant expertise, processes, and key personnel that would support the CLA IoT Labeling Program requirements and responsibilities.

[123] In addition to demonstrating the relevant controls in place to avoid conflicts of interest, Applicants may also provide prior experience in avoiding personal and organizational conflict (e.g., history of, processes for, working with, certification labs on an equitable basis. *See* ISO/IEC 17065, § 4.2.2 Management of Impartiality ("The certification body shall be responsible for the impartiality of its certification activities and shall not allow commercial, financial or other pressures to compromise impartiality.").

[124] Applicants may describe existing data systems, personnel and other resources, processes (e.g., record-keeping etc.) in place or to be developed, for reviewing, accepting or denying applications to use the FCC IoT label in accordance with ISO/IEC 17065.

[125] For example, Applicants may describe their experience with the FCC's Equipment Authorization Program or another FCC-run compliance program. *See* 47 CFR part 2.

[126] *See, e.g.*, FISMA; Freedom of Information Act (FOIA); and the Open, Public, Electronic, and Necessary Government Data Act (OPEN Government Data Act).

following:[127]

a. Obtaining accreditation pursuant to all of the requirements associated with ISO/IEC 17065 with the forthcoming FCC program scope;[128]

b. The ability (*e.g.*, appropriate testing equipment, and personnel with the necessary technical expertise and training) to conduct post-market surveillance activities, such as audits, in accordance with ISO/IEC 17065;

c. Implementation of a process for receiving complaints alleging an IoT product does not support the cybersecurity criteria conveyed by the Cyber Trust Mark and referring those complaints to the Lead Administrator;

d. Collaborating with the Lead Administrator and other stakeholders to develop those items to be submitted to the Commission within 90 days of election of the Lead Administrator, and listed in 47 CFR § 8.221(a)(4); and

e. Being an active participant in the consumer education campaign led by and in coordination with the Lead Administrator.

B. Applications for Lead Administrator

36. In addition to the above requirements for CLA applications, Lead Administrator applicants must demonstrate the following:

a. Description of Applicant's previous experience in IoT cybersecurity;[129]

b. Description of Applicant's previous roles, if any, in IoT labeling;[130]

c. Description of Applicant's capacity (e.g., available resources, systems, infrastructure etc.), and commitment to execute the following Lead Administrator duties:[131]

i. Interfacing with the Commission on behalf of CLAs, which includes but is 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;

ii. Conducting stakeholder outreach, coordinating with CLAs and other stakeholders, and moderating stakeholder meetings;

---

[127] *See IoT Labeling Order* at 33-34, para. 59. CLAs must also comply with all requirements enumerated in 47 CFR § 8.220.

[128] *E.g.*, For purposes of conditional approval, applicants may meet this requirement by demonstrating they are certified to ISO/IEC 17065 under another scope. Alternatively, Applicants may outline a plan to receive ISO/IEC 17065 accreditation within six months of the effective date of the standards and testing procedures to be adopted under the forthcoming FCC program scope and demonstrate that their current or planned product testing processes align with ISO/IEC 17065. Each CLA must obtain 17065 accreditation to the FCC scope before it will be recognized by the Commission and authorized to begin processing applications to certify use of the FCC IoT Label.

[129] Where an Applicant describes previous experience or roles in IoT cybersecurity or IoT labeling, it may also describe how it expects to apply such previous experience to meet the Lead Administrator responsibilities.

[130] *E.g.*, Applicant may show a history of certifying IoT devices to a specific set of cybersecurity requirements. Alternatively, Applicant may show a history of certifying non-IoT devices to a designated cybersecurity scope.

[131] *See* 47 CFR § 8.221. Applicant may demonstrate relevant past experience, or otherwise provide a detailed plan to meet, each of the duties listed.

iii. Accepting, reviewing, and approving or denying 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 maintaining a publicly available list of Lead Administrator-recognized labs and a publicly available list of labs that have lost their recognition;

iv. Within 90 days of selection as Lead Administrator, in collaboration with the CLAs and other stakeholders (e.g., cyber experts from industry, government, and academia) submitting to the Bureau:

a) 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;

b) 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;

c) A recommendation on procedures for post market surveillance by the CLAs;

d) 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; and

e) Recommendations with regard to updates to the registry including whether the registry should be in additional languages, and if so, to recommend specific languages for inclusion.

d. Recommending appropriate modifications to the IoT Labeling Program standards and testing procedures within 45 days of publication of updates or changes to the NIST guidelines, or adoption by NIST of new guidelines, to stay aligned with NIST guidelines;

e. Developing, in collaboration with CLAs and other stakeholders, a consumer education campaign, submitting the consumer education plan to the Bureau, and participating in consumer education;

f. Receiving complaints about the Labeling Program, including but not limited to consumer complaints about the registry and coordinating with manufacturers to resolve any technical problems associated with consumers accessing the information in the registry;

g. Facilitating coordination between CLAs; and

h. Submitting to the Commission any other reports upon request of the Commission or as required by Commission rule.

i. Any additional information Applicant believes demonstrates why they should be designated the Lead Administrator.

C. Required Certification Statements

37. All applications MUST include the following certification statements under penalty of perjury[132] or they will be dismissed:

a. Applicant certifies that all statements made in this application and in the exhibits, attachments, or documents incorporated by reference are material, are part of this application, and are true, complete, correct, and made in good faith, see 47 CFR §§ 1.17, 8.220, 8.221.

b. 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. *See* 47 CFR § 1.2002(b) for the definition of "party to the application" as used in this certification.

c. The Applicant certifies that it is not delinquent on any debts to the Commission, see 47 CFR § 1.1910.

d. Applicant acknowledges that willful false statements made on the application or on any attachments are punishable by fine and/or imprisonment (U.S. Code, Title 18, § 1001) and/or forfeiture (U.S. Code, Title 47, § 503).

D. The application must be signed and dated.

38. The Application must be signed and dated by the individual authorized to sign on behalf of the Applicant.[133] **FAILURE TO SIGN THE APPLICATION MAY RESULT IN DISMISSAL OF THE APPLICATION.**

E. Application Submission.

39. The Bureau expects CLA and Lead Administrator applications and supporting documentation to be filed confidentially. Each page of the application must be clearly and conspicuously labeled "**CONFIDENTIAL, NOT FOR PUBLIC INSPECTION**." Applicant must file an original and one copy of each filing and supporting materials with the Office of the Secretary. All filings must reference **PS Docket No. 23-239** and be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission. Filings can be sent by hand or messenger delivery by commercial overnight courier, or First-Class or overnight U.S. Postal Service mail.

- All hand-delivered or messenger-delivered paper filings for the Commission's Secretary are accepted between 8:00 a.m. and 4:00 p.m. 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 overnight deliveries (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
- U.S. Postal Service First-Class, Express, and Priority mail must be sent to 45 L Street NE, Washington, DC 20554.

---

[132] *See* 47 CFR § 1.16.

[133] *See* 47 CFR § 1.52 ("If filed electronically, a signature will be considered any symbol executed or adopted by the party with the intent that such symbol be a signature, including symbols formed by computer-generated electronic impulses.").

40. An electronic version of the application and supporting material is required to be submitted to FCC staff as a .pdf file via email to CyberTrustMark@fcc.gov. **The document must be password protected and the password communicated in a separate email to** CyberTrustMark@fcc.gov. Submissions may be broken into multiple emails when necessary.

41. Applications should be received by the Commission as soon as possible, but no later than October 1, 2024. Applicants requiring additional time may request an extension of time for up to 10 additional calendar days to complete their applications. Applications received after October 1, 2024 from an entity that has not been approved an extension of time, will not be accepted and will be dismissed. Procedures for submitting applications are set forth below.

F. Additional Instructions to Assist with CLA and/or Lead Administrator Applications

- **Instructions.** General filing instructions are available in Appendix A.
- **Frequently Asked Questions (FAQs).** The FAQs are available at https://www.fcc.gov/CyberTrustMark.
- **FCC Notice Required by the Paperwork Reduction Act.** The FCC Notice Required by the Paperwork Reduction Act is available in Appendix D.
- **Privacy Act Statement.** The Privacy Act Statement is available in Appendix E.
- **Requirement for an FCC Registration Number (FRN).** We remind all applicants that they must have an FRN to file their applications. An FRN is the 10-digit number assigned to all individuals and entities that transact business with the Commission,[134] and it must be provided any time an applicant submits or updates their application.
- **Applicant Does Not Have an FRN.** If an applicant does not have an FRN, the applicant must obtain an FRN through the Commission Registration System (CORES) webpage at https://apps.fcc.gov/cores/userLogin.do.
    - For additional assistance, submit a help request at https://www.fcc.gov/wireless/available-support-services or call the FRN Help Desk at (877) 480-3201 (Monday-Friday, 8 a.m.-6 p.m. ET).
    - If the applicant has further questions, an email can be sent to CyberTrustMark@FCC.gov.
- **Applicant has an FRN.** If an applicant has an FRN, the applicant must use that FRN with its application.
    - The applicant should not obtain a new FRN if Applicant already has an FRN.
    - An applicant can identify its FRN by accessing records the Commission's Registration Systems (CORES)[135] and click "Search". Individuals can search by

[134] 47 CFR § 1.8002(a) ("The FRN must be obtained by anyone doing business with the Commission, see 31 U.S.C. § 7701(c)(2) . . . .").

[135] FCC User Registration System, available at https://apps2.fcc.gov/fccUserReg/pages/login.htm https://apps2.fcc.gov/fccUserReg/pages/login.htm (last accessed Aug. 15, 2024).

name, or contact related information. Business organizations can search by name, Employer Identification Number (EIN), or contact-related information.

V. NEXT STEPS

42. After the application filing window closes October 1, 2024, the Bureau will review and evaluate properly filed applications. **The Bureau's selection of CLAs and a Lead Administrator will be announced by public notice.** The Public Notice will describe the next steps for selected entities, including but not limited to the execution of a licensing agreement and/or other appropriate documentation governing the details of the CLAs' and Lead Administrator's responsibilities and relationship to the Commission.[136]

VI. PROCEDURAL MATTERS

43. *Regulatory Flexibility Act*. The Regulatory Flexibility Act of 1980, as amended (RFA),[137] 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."[138] Accordingly, we have prepared a Supplemental Final Regulatory Flexibility Analysis (Supplemental FRFA) concerning the possible impact of the rule changes contained in this Public Notice on small entities. The Supplemental FRFA is set forth in Appendix C.

44. *Paperwork Reduction Act.* This document contains modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. It will be submitted to the Office of Management and Budget (OMB) for review under Section 3507(d) of the PRA. OMB, the general public, and other Federal agencies will be invited to comment on the new or modified information collection requirements contained in this proceeding. In addition, we note that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 44 U.S.C. § 3506(c)(4), we previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees.

45. In this present document, we have assessed the effects of requiring CLAs to develop and implement a cybersecurity risk management plan identifying the cyber risks that the entity faces, the controls used to mitigate those risks, and the steps taken to ensure that these controls are applied effectively to their operations. The plans must also describe how the CLA employs its organizational resources and processes to ensure the confidentiality, integrity, and availability of its information and information systems and find that Since applying to be a CLA is voluntary, small entities who do not apply to be a CLA will not be subject to any new or modified reporting, recordkeeping, or other compliance obligations. Small entities that choose to apply to be a CLA, and whose applications are approved by the Bureau, will incur recordkeeping and reporting as well as other obligations to comply with the requirements we adopt in this Public Notice. We find that, for the FCC's IoT Labeling Program to have meaning for consumers, CLA requirements must be uniform for both small businesses and other entities. Thus, significance of program integrity, and building confidence among consumers that devices and products containing the Cyber Trust Mark label can be trusted to be cyber secure, necessitates adherence by all entities participating in the IoT Labeling Program to the same rules regardless of size.

---

[136] *See IoT Labeling Order* at 36, para. 64.

[137] 5 U.S.C. § 603.

[138] 5 U.S.C. § 605(b).

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

47. *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 & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (TTY).

48. *Additional Information.* For further information regarding this proceeding, please contact Drew Morin, Deputy Division Chief, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau by email to Drew.Morin@fcc.gov or 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.

VII. ORDERING CLAUSES

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

50. IT IS FURTHER ORDERED that the amendments of the Commission's Rules as set forth in Appendix B are ADOPTED, effective 30 days after publication in the Federal Register, except for the amendment to 47 CFR § 8.220(f)(14). The amendment to 47 CFR § 8.220(f)(14), which may contain modified information collection requirements, will not become effective until OMB completes any review that the Public Safety and Homeland Security Bureau determines is required under the Paperwork Reduction Act. The Public Safety and Homeland Security Bureau will announce effective dates for this section by publication in the Federal Register and by subsequent Public Notice.

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

52. IT IS FURTHER ORDERED that the Office of the Managing Director, Performance Program Management, SHALL SEND a copy of this *Public Notice* in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act, *see* 5 U.S.C. § 801(a)(1)(A).

APPENDIX A

GENERAL FILING INSTRUCTIONS

A. Provide All Information Requested: Applicants should provide all information requested by the application. If any portion of an application is not applicable, the applicant should so state. **Defective or incomplete applications will be returned without consideration.** Inadvertently accepted applications are also subject to dismissal.

B. 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. *See* 47 C.F.R. § 1.65.

C. Applicable Rules and Regulations: Applicants should obtain the relevant parts of the FCC's rules in Title 47 of the Code of Federal Regulations. Copies of Title 47 may be purchased from the Superintendent of Documents; Government Printing Office; Washington, DC 20402; (202) 512-1800. Refer also to the Government Printing Office's website at http://www.access.gpo.gov. Some FCC Rules require the Applicant to attach one or more exhibits to an application in addition to the information requested in the application form.

D. Exhibits: Each document required to be filed as an exhibit should be current as of the date of the filing. Each page of every exhibit must be identified with the number or letter of the exhibit, and the total number of pages of the exhibit.

E. Confidentiality: Applications will be treated as presumptively confidential under the Commission's rules.

F. Explanatory Exhibits: Applicants may submit explanations and exhibits where necessary or appropriate. An inability to fully demonstrate satisfaction of all of the listed requirements will not cause *immediate* dismissal of the application provided that an explanatory exhibit is submitted.

G. Applicant Information: Applicant Name, Type, and Contact Information: The name of an applicant must be stated exactly. If the applicant is a corporation, the exact corporate name; if a partnership, the name under which the partnership does business; if an unincorporated association, the name of an executive officer, his/her office, and the name of the association; and, if an individual applicant, the person's full legal name. Applicants should use only those state abbreviations approved by the U.S. Postal Service.

H. Contact Representatives: If the applicant is represented by a third party (for example, legal counsel) that will be engaging with the Commission related to its application, that person's name, firm or company, mailing address and telephone/electronic mail address must be specified.

I. Signature: The application must be signed by a person authorized to sign applications on behalf of the applicant and include that person's title. The signature certifies that all information provided on the application is true and correct and that the undersigned is in compliance with all of the General Certification Statements. Applications and amendments must be signed in accordance with part 1 of the FCC rules. The signor must be a person authorized by the applicant to sign the application.

J. False Statements: Willful false statements made in the application or any attachments are punishable by fine and/or imprisonment (U.S. Code, Title 18, Section 1001) and/or forfeiture (U.S. Code, Title 47, Section 503).

APPENDIX B

FINAL RULES

For the reasons set forth above, Part 8 of Title 47 of the Code of Federal Regulations is amended as follows:

Part 8 – SAFEGUARDING AND SECURING THE INTERNET

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

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

Subpart B—Cybersecurity Labeling Program for IoT Products

2. Add § 8.220(f)(12) – (14) as follows:

§ 8.220 Requirements for CLAs.

(12) A CLA shall share the Lead Administrator's expenses incurred as a result of the Lead Administrator's performance of its duties under the FCC IoT Labeling Program.

(i) The Lead Administrator expenses subject to sharing by CLAs are those expenses determined to be reasonable by the Public Safety and Homeland Security Bureau and the Office of Managing Director.

(ii) A CLA shall share Lead Administrator expenses pursuant to a methodology agreed to by the CLAs and the Lead Administrator subject to ongoing oversight by the Commission.

(13) A CLA shall maintain the confidentiality of non-public information received as part of an application for authority to use the FCC IoT Label, and will implement appropriate administrative, technical, procedural, and physical safeguards to protect the confidentiality of information received by the CLA and protect against the unauthorized disclosure and unauthorized use of non-public information received as a result of its participation in the FCC IoT Labeling Program.

(14) A CLA shall create, update, and implement a cybersecurity risk management plan identifying the cyber risks that the entity faces, the controls used to mitigate those risks, and the steps taken to ensure that these controls are applied effectively to their operations. The plan must also describe how the CLA employs its organizational resources and processes to ensure the confidentiality, integrity, and availability of its information and information systems. The CLA's cybersecurity risk management plan must be available to the Commission upon request.

3. Add § 8.221(a)(11) – (14) as follows:

§ 8.221 Requirements for the Lead Administrator.

(11) Create, update, and implement a cybersecurity risk management plan identifying the cyber risks that the entity faces, the controls used to mitigate those risks, and the steps taken to ensure that these controls are applied effectively to their operations. The plan must also describe how the Lead Administrator employs its organizational resources and processes to ensure the confidentiality, integrity, and availability of its information and information systems. The Lead Administrator's cybersecurity risk management plan must be available to the Commission upon request;

(12) Submit to the Public Safety and Homeland Security Bureau and the Office of the Managing Director, an estimate of its forward-looking costs including, separately, program stand-up costs and ongoing program costs to perform the Lead Administrator duties for the Lead Administrator's upcoming calendar year, which will be reviewed by the Cybersecurity Labeling Administrators, Public Safety and Homeland Security Bureau, and the Office of the Managing Director for reasonableness, and if reasonable, will be used to estimate the overall CLA cost sharing obligation;

(13) Implement internal controls adequate to ensure its operations maintain best practices to protect against improper payments and to prevent fraud, waste, and abuse in its handling of funds; and

(14) Submit to the Public Safety and Homeland Security Bureau and the Office of the Managing Director, an annual, independently audited, statement of program expenditures and monies received from the CLAs due before the end of the Lead Administrator's calendar year.

APPENDIX C

Supplemental Final Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] a Supplemental Initial Regulatory Flexibility Analysis (Supplemental IRFA) was incorporated in the *Public Safety and Homeland Security Bureau Requests Comment on Implementation of the Cybersecurity Labeling for Internet of Things Program* Public Notice (*June 2024 IoT Labeling Public Notice*) released in June 2024.[2] The Public Safety and Homeland Security Bureau (Bureau) sought written public comment on the proposals in the *June 2024 IoT Labeling Public Notice*, including comment on the IRFA. No comments were filed addressing the Supplemental IRFA. This Supplemental Final Regulatory Flexibility Analysis (Supplemental FRFA) reflects actions taken in this *Public Notice*, and supplements the Final Regulatory Flexibility Analysis completed by the Federal Communications Commission (Commission or FCC) in the *Cybersecurity Labeling for Internet of Things* Report and Order and Further Notice of Proposed Rulemaking (*IoT Labeling Order*). This present Supplemental FRFA conforms to the RFA.[3]

A. Need for, and Objectives of, the Public Notice

2. In the *IoT Labeling Order*, adopted in March 2024, the Commission established a framework for a voluntary cybersecurity labeling program for consumer wireless Internet of Things (IoT) products (IoT Labeling Program),[4] which includes selecting third party administrators to support the program.[5] The Commission delegated authority to the Bureau to open an initial filing window to receive applications from entities seeking authority to be recognized as a CLA (Cybersecurity Labeling Administrator*)* and those seeking to be recognized as the Lead Administrator.[6] CLAs approved by the Commission will authorize use of the FCC IoT Label, which includes the U.S. government certification mark (U.S. Cyber Trust Mark), by manufacturers whose products are found to be in compliance with the Commission's IoT cybersecurity labeling program rules.[7] The Lead Administrator will, among other duties, act as liaison between the Commission and CLAs, conduct stakeholder outreach to identify and/or develop and recommend to the Bureau technical standards and testing procedures for at least one class of IoT products, and in collaboration with CLAs, the FCC, and other stakeholders develop and execute a plan for a consumer education campaign.[8]

3. In today's Public Notice, the Bureau addresses comments filed in response to the Bureau's proposals in the *June 2024 IoT Labeling Public Notice* to further the efficient and timely rollout of the

---

[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 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[2] *Public Safety and Homeland Security Bureau Requests Comment on Implementation of the Cybersecurity Labeling for Internet of Things Program*, PS Docket No. 23-239, DA 24-617 (June 27, 2024) (*June 2024 IoT Labeling Public Notice*).

[3] 5 U.S.C. § 604.

[4] *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*).

[5] *IoT Labeling Order* at 26, para. 48.

[6] *Id.* at 36, para. 64. The *IoT Labeling Order* also delegated authority to the Bureau to open additional filing windows or otherwise accept additional applications for authority to be recognized by the Bureau as a CLA when and as the Bureau determines it is necessary. *Id.*

[7] *Id*. at 26-27, para. 48.

[8] *Id*. at 27-29, para. 52.

IoT Labeling Order and IoT Labeling Program. The Bureau announces that the 15-business day filing window for applications from entities seeking designation by the Commission as a CLA and Lead Administrator **will open on September 11, 2024 and close on October 1, 2024**. The Bureau also provides determinations regarding application format, filing fees, selection criteria, and Lead Administrator neutrality, and adopts rules regarding CLA sharing of Lead Administrator program costs, confidentiality of information CLA receives, creation and implementation of cybersecurity risk management plans by CLAs and the Lead Administrator, and the requirement that the Lead Administrator implement internal controls to prevent fraud, waste, and abuse in its handling of funds, and submit an annual audited statement of program expenditures and monies received from CLAs.

4. To encourage manufacturer participation in the IoT Labeling Program and safeguard proprietary technology and trade secrets, in the Public Notice we adopt requirements for CLAs, including the Lead Administrator, to maintain the confidentiality of non-public information received as part of an application for authority to use the FCC IoT Label, and implement appropriate administrative, technical, procedural, and physical safeguards to protect the confidentiality of information received by the CLA, and protect against the unauthorized disclosure and unauthorized use of non-public information received as a result of its participation in the FCC IoT Labeling Program. Additionally, we require CLAs, including the Lead Administrator, to create, update, and implement a cybersecurity risk management plan identifying the cyber risks that the entity faces, the controls used to mitigate those risks, and the steps taken to ensure that these controls are applied effectively to their operations. We also require the Lead Administrator to implement financial controls, which will further increase the integrity of the program by ensuring the Lead Administrator's costs, which are to be shared among the CLAs, are estimated in advance and evaluated for reasonableness, and ensuring the Lead Administrator is a good steward of funds it receives from CLAs to support its role as Lead Administrator.

5. The IoT Labeling Program 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. Consumer IoT products are susceptible to a wide range of security vulnerabilities that can be exploited by attackers to gain unauthorized access to the IoT product and its data. Providing customers with an easy-to-understand label indicating that an IoT product has satisfied baseline cybersecurity standards allows them to understand the relative security risk that an IoT product may pose when making a purchase.

B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

6. There were no comments filed that specifically address the proposed rules and policies in the IRFA.

C. Response to Comments by the Chief Counsel for Advocacy of the Small Business Administration

7. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA, the Commission is required to respond to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration (SBA) and to provide a detailed statement of any change made to the proposed rules as a result of those comments.[9] The Chief Counsel did not file any comments in response to the proposed rules in this proceeding.

[9] 5 U.S.C. § 604(a)(3).

D. Description and Estimate of the Number of Small Entities to Which the Rules Will Apply

8. The RFA directs agencies to provide a description of and, where feasible, an estimate of, the number of small entities that may be affected by the rules, adopted herein.[10] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[11] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[12] 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.[13]

9. As noted above, a regulatory flexibility analysis was incorporated into the *IoT Labeling Order*. The *IoT Labeling Order* provides the underlying authority for the procedures proposed in the *June 2024 IoT Labeling Public Notice*, and that are adopted in today's Public Notice for the IoT Labeling Program. In the *IoT Labeling Order* regulatory flexibility analysis, the Commission described in detail the small entities that might be significantly affected. Accordingly, in this Supplemental FRFA, we hereby incorporate by reference the descriptions and estimates of the number of small entities from the previous regulatory flexibility analysis in the *IoT Labeling Order*.

E. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

10. The Commission's *IoT Labeling Order* adopted the operational framework for a voluntary IoT cybersecurity labeling program. The IoT Labeling Program framework incorporates, and is consistent with, certain National Institute of Standards and Technology (NIST) guidelines and protocols as part of the Commission's recognition that public-private collaboration that leverages the expertise and existing frameworks of the federal government, industry, and other stakeholders is necessary for the success of its voluntary IoT Labeling Program. The Commission will be the IoT Labeling Program owner and retain ultimate control over the IoT Labeling Program, however, CLAs and the Lead Administrator will carry out responsibilities such as management of day-to-day functions, and development of processes, standards, and testing to be approved by the Commission. Since the IoT Labeling Program is voluntary, small entities who do not participate in the IoT Labeling Program will not be subject to any new or modified reporting, recordkeeping, or other compliance obligations. Moreover, small entities who do not wish to apply for selection as a CLA or Lead Administrator will also not be subject to any new or modified compliance obligations arising from today's Public Notice. Those small entities that choose to participate in the IoT Labeling Program by applying for selection as a CLA, or the Lead Administrator will incur recordkeeping, reporting, and other compliance obligations in the course of applying and, if selected, carrying out the responsibilities required in the *IoT Labeling Order*.[14]

---

[10] *Id.* § 604(a)(4).

[11] 5 U.S.C. § 601(6).

[12] 5 U.S.C. § 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."

[13] 15 U.S.C. § 632.

[14] *See IoT Labeling Order* at 27-32, paras. 51-58.

11. The *IoT Labeling Order* contemplated that small entities may choose to file applications for the roles of CLA and Lead Administrator, which today's Public Notice clarifies will be in the form of a narrative application demonstrating their relevant qualifications and experience as set out in the *IoT Labeling Order*,[15] and the application procedures adopted in today's Public Notice. In accordance with our determination that a CLA and Lead Administrator application and supporting documentation will be treated as presumptively confidential, each page of an applicant's submission must be clearly and conspicuously labeled "**CONFIDENTIAL, NOT FOR PUBLIC INSPECTION**." CLA and Lead Administrator applications must be filed with the Office of the Secretary either via hand or messenger delivery, by commercial overnight courier, or First-Class or overnight U.S. Postal Service mail. A copy of the application and supporting documentation must be sent to the Bureau via email in a password protected .pdf file. Applications must be signed and dated by the individual authorized to sign on behalf of the Applicant, and must certify that all statements made in the application and any accompanying exhibits, attachments, or documents incorporated by reference are material, are part of the application, and are true, complete, correct, and made in good faith.[16] Applicants must also certify 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,[17] that the Applicant is not delinquent on any debts to the Commission,[18] and that the Applicant acknowledges that willful false statements made on the application or on any attachments are punishable by fine and/or imprisonment and/or forfeiture.[19]

12. If selected to be a CLA or the Lead Administrator, small entities and others will be required to create, update, and implement a cybersecurity risk management plan identifying the cyber risks that the entity faces, the controls used to mitigate those risks, and the steps taken to ensure that these controls are applied effectively to their operations. The plan must also describe how the CLA employs its organizational resources and processes to ensure the confidentiality, integrity, and availability of its information and information systems. The CLA's cybersecurity risk management plan must be available to the Commission upon request. If selected to be the Lead Administrator, the selected entity will also be required to submit to the Bureau, and the Office of the Managing Director (OMD), an estimate of its forward-looking costs including, separately, program stand-up costs and ongoing program costs to perform the Lead Administrator duties for the Lead Administrator's upcoming calendar year; implement internal controls adequate to ensure its operations maintain best practices to protect against improper payments and to prevent fraud, waste, and abuse in its handling of funds; and submit to the Bureau and OMD, an annual, independently audited, statement of program expenditures and monies received from the CLAs due before the end of the Lead Administrator's calendar year.

13. Regarding compliance costs for small entities that could result from the requirements adopted in today's Public Notice, the record does not include sufficient cost information to allow the Commission to quantify the costs of compliance for small entities, including whether it will be necessary for small entities to hire professionals to comply. The Bureau notes however, we reduce the cost of the application process for small and other CLA or the Lead Administrator applicants by not imposing the application fees we contemplated in the *June 2024 IoT Labeling Public Notice.* We also note the requirement for selected CLAs and Lead Administrators to create, implement and submit a cybersecurity risk management plan gives small and other entities the flexibility to structure its cybersecurity risk

---

[15] *See IoT Labeling Order* at 32-35, paras. 59-62; 47 CFR §§ 8.220(c); 8.221(b).

[16] *See* 47 CFR §§ 1.17, 8.220, 8.221.

[17] *See* 47 CFR § 1.2002(b) for the definition of "party to the application" as used in this certification.

[18] *See* 47 CFR § 1.1910.

[19] *See* 18 U.S.C. § 1001; 47 U.S.C. § 503.

management plan based on its operational and financial needs, as long as that the plan demonstrates that the entity is taking affirmative steps to analyze security risks and improve its security posture. Further small and other entities have the ability to utilize industry established and recognized, scalable and adaptable risk management frameworks to meet our requirements. Therefore, the Bureau does not anticipate that small entities serving as a CLA or the Lead Administrator will need to hire outside cybersecurity consultants or other professionals to comply with the cybersecurity risk management plan requirements adopted in today's Public Notice. CLAs and Lead Administrators should be able to develop their risk management plans without hiring specialized consultants based on how they currently identify cybersecurity risks, the controls used to mitigate those risks, and the methods used to ensure that these controls are effective.

F. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

14. The RFA requires an agency to provide, "a description of the steps the agency has taken to minimize the significant economic impact on small entities…including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected."[20]

15. The Bureau has taken steps to minimize the economic impact of our IoT Labeling Program requirements as a general matter, and in some cases, for small entities, specifically. As mentioned in the previous section, the Bureau declined to adopt the filing fee for CLA ($1,520) and Lead Administrator ($2,290) applications that we proposed in the *June 2024 IoT Labeling Public Notice*. Moreover, application filing procedures required in today's Public Notice build on a framework for filing confidential materials that the Commission has used in the past which small entities may already be familiar with and have utilized.[21] Further, maintaining the presumptive confidentiality of applications filed in the CLA and Lead Administrator application process the Bureau will protect the economic interests of small entities' and others' proprietary technology and trade secrets. Additionally, to aid in the creation of CLA and Lead Administrator applications, the Bureau has also offered a number of examples of criteria that can be used to comply with the application requirements enumerated in today's Public Notice. Applicants whose applications require further attention may communicate with the Bureau to provide additional information or clarification as needed to complete their application.

16. The Bureau's decision to require cybersecurity risk management plans based on established risk management frameworks such as the NIST Cybersecurity Framework or Risk Management Framework will also minimize the economic impact on small and other entities selected to serve as CLAs or the Lead Administrator. Small entities will likewise benefit economically from the Bureau's decision to reconsider our tentative conclusion in the *June 2024 IoT Labeling Public Notice* to apply the Federal Information Security Modernization Act of 2014 (FISMA) to CLAs and the Lead Administrator, and decline to require compliance with FISMA, which would have been significantly more burdensome for small entities. The Bureau also considered but declined to adopt additional selection criteria for CLA and Lead Administrator applicants, or additional safeguards to ensure the stakeholder process remains competitively neutral beyond the requirements adopted in the *IoT Labeling Order*.

G. Report to Congress

---

[20] 5 U.S.C. § 604(a)(6).

[21] *See, e.g.*, *FCC Provides Further Instructions Regarding Submission of Confidential Materials*, Public Notice, DA 20-361 (Mar. 31, 2020).

17. The Commission will send a copy of the *Public Notice*, in a report to Congress pursuant to the Congressional Review Act.[22] In addition, the Commission will send a copy of the *Public Notice*, including the Supplemental FRFA, to the Chief Counsel for Advocacy of the SBA. A copy of the *Public Notice* and FRFA (or summaries thereof) will also be published in the *Federal Register*.[23]

[22] 5 U.S.C. § 801(a)(1)(A).

[23] *Id.* § 604(b).

Approved by OMB

OMB Control Number 3060-1328

July 2024

Estimated Time per Response – 14 hours

APPENDIX D

FCC NOTICE REQUIRED BY THE PAPERWORK REDUCTION ACT

The public reporting for this collection of information is estimated to average 20 hours per CLA response and 10 additional annual burden hours per Lead Administrator response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the required data, and completing and reviewing the collection of information. If you have any comments on this burden estimate, or how we can improve the collection and reduce the burden it causes you, please write to the Federal Communications Commission, AMD−PERM, Paperwork Reduction Project (3060-1328), Washington, DC 20554. We will also accept your comments regarding the Paperwork Reduction Act aspects of this collection via the Internet if you send them to PRA@fcc.gov. **PLEASE DO NOT SEND COMPLETED APPLICATIONS TO THIS ADDRESS.**

Remember − You are not required to respond to a collection of information sponsored by the Federal government, and the government may not conduct or sponsor this collection, unless it displays a currently valid OMB control number or if we fail to provide you with this notice. This collection has been assigned an OMB control number of 3060-1328.

THE FOREGOING NOTICE IS REQUIRED BY THE PAPERWORK REDUCTION ACT OF 1995, PUBLIC LAW 104−13, OCTOBER 1, 1995, 44 U.S.C. SECTION 3507.

Approved by OMB

OMB Control Number 3060-1328

July 2024

Estimated Time per Response – 14 hours

APPENDIX E

PRIVACY ACT STATEMENT

Authority: The FCC is authorized to collect the information pursuant to the authority contained in sections 1, 2, 4(i), 4(n), 302, 303(r), 312, 333, and 503, of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152, 154(i), 154(n), 302a, 303(r), 312, 333, 503; the IoT Cybersecurity Improvement Act of 2020, 15 U.S.C. § 278g-3a to § 278g-3e.

Purpose: The information collected in this Application includes contact and certification information from entities voluntarily applying to serve as Lead Administrator or CLA in this FCC program. The information is used to communicate with such entities and enforce their compliance with statements made in their applications.

Routine Uses: While Lead Administrator and CLA applications will be presumed confidential, in addition to those disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended, the FCC may disclose contact and certification information collected from applicants as is determined to be relevant and necessary, outside the FCC as a routine use pursuant to 5 U.S.C. § 552a(b)(3), including: to authorized third parties to administer, support, participate in, or receive information related to FCC programs and activities; to other Federal agencies in order to administer, support, participate in, or receive information related to FCC programs and activities; and to non-federal personnel, including contractors, who have been engaged to assist the FCC in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity.

A full, detailed list of the routine uses is published in the system of records notice associated with this collection, FCC-2, Business Contacts and Certifications, which is available at https://www.fcc.gov/sites/default/files/sor-fcc-2.pdf.

Disclosure: This information collection is voluntary. The Public Safety and Homeland Security Bureau's Public Notice provides entities the opportunity to apply to be designated a Cybersecurity Labeling Administrator and the opportunity to apply to be designated a Lead Administrator.