FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Public Safety and Homeland Security	)	PS Docket No. 23-239
Bureau Requests Comment on	)	
Implementation of the Cybersecurity	)	
Labeling for Internet of Things Program	)	

Relating to the
Notice of Proposed Rulemaking
Issued July 18, 2024

Reply Comments of

Electronic Privacy Information Center

September 3, 2024

By:
Chris Frascella
Counsel
frascella@epic.org
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, D.C. 20036

Comments

I. Introduction and Summary

The **Electronic Privacy Information Center (EPIC)**[1] submits this reply comment to supplement the joint comments that were filed by EPIC and others on August 19, 2024[2] in the Public Safety and Homeland Security Bureau's (PSHSB's or Bureau's) Request for Comment regarding "Implementation of the Cybersecurity Labeling for Internet of Things Program" published in the Federal Register on July 18, 2024.[3]

EPIC believes it is essential for the Bureau to provide robust oversight, accountability, and transparency for the standard-setting and product certification process to ensure that the U.S. Cyber Trust Mark protects consumers. The selection of the Lead Administrator implicates these three priorities;[4] additionally the Bureau should address potential conflict of interest issues between the Cybersecurity Label Administrators (CLAs) and the Lead Administrator, as well as ensure adequate enforcement for wrongly-applied labels.

II. The Bureau should ensure that the standards setting process is transparent and open to stakeholder participation from consumer groups to ensure that the U.S. Cyber Trust Mark serves its purpose.

We support the Bureau's proposals that the standards, testing criteria, and label design be stakeholder consensus-based, but urge that the relevant stakeholder entities should include representatives from consumer advocacy groups and not merely include representatives from industry groups, and that the process be transparent.[5] Researchers, consumer advocates, and tech-

[1] Electronic Privacy Information Center (EPIC) is a public interest research center established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.
[2] Comments of Consumer Reports, Carnegie Mellon University, Public Knowledge, Electronic Privacy Information Center, New York University, PSHSB 23-239 (Aug. 19, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10819759410275 [hereinafter "Comments of Consumer Reports et al"].
[3] Public Safety and Homeland Security Bureau Requests Comment on Implementation of the Cybersecurity Labeling for Internet of Things Program, Proposed Rule, 89 Fed. Reg. 58312 (July 18, 2024), https://www.federalregister.gov/documents/2024/07/18/2024-15379/public-safety-and-homeland-security-bureau-requests-comment-on-implementation-of-the-cybersecurity [hereinafter "RFC"].
[4] *See, e.g.*, Comment of CTIA, PSHSB 23-239, at 11 (Aug. 19, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10819238529940 (CTIA noting that details of the post-market surveillance program may impact applications and selection of Lead Administrator).
[5] RFC at ¶ 13, *available at* https://www.federalregister.gov/d/2024-15379/p-42; others also explicitly support this approach. *See* Comment of Meghan Housewright (UL), PSHSB 23-239, at 4 (Aug. 19, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10819106738061.

savvy consumers should be able to understand and evaluate the threshold standard that must be met for a product to earn the U.S. Cyber Trust Mark (Trust Mark). Consumers should feel confident in the process for determining whether a product meets that standard. In Section III immediately below, we focus on issues of compliance, operating from the assumption that the standards set by this stakeholder process will accurately determine whether a product is adequately secure to merit its displaying the Trust Mark. This is more likely to occur if the Bureau directs the Lead Administrator to give weight to the input of consumer advocates in the Lead Administrator's development of the Trust Mark's standards, because consumer advocates necessarily prioritize preventing consumer harm whereas industry representatives, while they may consider their own reputational interests and consumer interests, necessarily consider and likely prioritize financial impacts.[6]

III. Oversight and accountability are the *sine qua non* of a voluntary cybersecurity labelling program meant to develop consumer trust.

The Trust Mark program will only be effective if it supports consumer confidence in the security of labeled products, and if there are adequate oversight and accountability measures to ensure that products are and continue to be in compliance. Complaints[7] and post-market surveillance[8] can provide some accountability, but there must be an ongoing oversight processes that prevent products from being wrongfully introduced into the marketplace with a label in the first instance. For example, there should be strong incentives that discourage a CLA from approving a product to display the Trust Mark if that product does not actually meet the program's threshold requirements.[9] In this regard, the Bureau must be responsible for answering who watches the watchmen—and how.

[6] The Commission declined to require that CLAs—which are responsible for measuring whether a given product satisfies the Trust Mark's minimum requirements—must be non-profit organizations, because it found that a for-profit organization could be neutral, knowledgeable, and free from conflicts. *See* Report and Order and Further Notice of Proposed Rulemaking, *In re* Cybersecurity Labeling for Internet of Things, at ¶ 62 (Mar. 15, 2024), https://docs.fcc.gov/public/attachments/FCC-24-26A1.pdf [hereinafter "R&O"]. The Lead Administrator however serves a different role, establishing the very shape of Trust Mark program's threshold requirements.
[7] *See, e.g.*, RFC at ¶ 16, *available at* https://www.federalregister.gov/d/2024-15379/p-45.
[8] *See, e.g.*, R&O at ¶¶ 125-28.
[9] At present this authority seems to rest with the Commission and the Bureau at the level of termination of CLA authority, but there is no explicit discussion of authority for interim or alternative interventions. *See, e.g.*, R&O at ¶ 63.

The Bureau needs a mechanism or mechanisms for compelling CLAs and the Lead Administrator to adhere to the goals and requirements of its program. As the Bureau implied, the mechanism to implement accountability measures may look different for different entities and in different factual contexts.[10] Because the Trust Mark is a voluntary program, merely revoking a CLA's status as such may not be adequate incentive to prevent CLAs from becoming complicit in granting certifications wrongfully, nor to prevent the Lead Administrator from neglecting its role in escalating complaints it receives about CLAs.[11] Numerous commenters have called attention to potential issues of conflict of interest between CLAs and the Lead Administrator,[12] and this is especially concerning where it may ultimately result in a consumer purchasing a product displaying the Trust Mark label when that product has not actually met the program's standards. Consumers purchasing products with the Trust Mark should not have to wonder or worry about whether those products are actually secure. The purpose of the label is to provide that assurance and there must be sufficient oversight of the CLAs and the Lead Administrator to ensure that they are setting and enforcing the standards.[13]

The Bureau has proposed a process for choosing a replacement Lead Administrator in the event that: the Lead Administrator requests being replaced, the Lead Administrator's accreditation is withdrawn, or if there is just cause for the Bureau withdrawing its approval of the Lead Administrator.[14] We encourage the Bureau to promote a system of independent monitoring and review to inform this selection process. A CLA that has accurately disputed another CLA's determination that a product meets the Trust Mark standards demonstrates the commitment to the program and attention to detail that a Lead Administrator should embody. Similarly, where a product that should not have been authorized to display the Trust Mark was approved by a

[10] *See* RFC at ¶ 16, *available at* https://www.federalregister.gov/d/2024-15379/p-45.
[11] *See id.*
[12] *See, e.g.*, Comment of NCTA – The Internet & Television Association, PSHSB 23-239, at 7 (Aug. 19, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10819301318524 (noting potential conflict of interest concerns); Comment of Somos at 3 (Aug. 19, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10819049743260; Comment of Infineon Technologies Americas Corp. at 3 (Aug. 19, 2024); Comment of TIC Council Americas at 2 (Aug. 19, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/1081976943825; Comment of A2LA at 2 (Aug. 19, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/1081999874923.
[13] We frame this issue in terms of harm to consumers, but it also implicates harm to competition more broadly, as the honest merchant should not be disadvantaged due to the misconduct of the dishonest merchant.
[14] *See* RFC at ¶ 14, *available at* https://www.federalregister.gov/d/2024-15379/p-43.

CLA,[15] that CLA should be subject to greater scrutiny by the Bureau before that CLA can be approved to replace the Lead Administrator. We encourage the Bureau to consider other methods by which it might prevent wrongful labelling ex ante rather than ex post.

Additionally, as we noted in our reply comments in November 2023,[16] unlike ENERGY STAR®, the Trust Mark is not meant to capture a product's compliance at a single point in time but rather must represent a product's continued compliance. Whomever is selected to serve as the Lead Administrator will be responsible for establishing and overseeing the post-market surveillance program.[17] This audit-based oversight function must be wholly independent from any entities that conducted the initial attestation of compliance,[18] especially if the auditor is also an employee of the company creating the product being evaluated.[19] For example, in the event that the Lead Administrator also serves as a CLA, this would mean that even the Lead Administrator's CLA sister organization would need to be subject to a third party auditor.[20] The Bureau might consider seeking a civil society partner to support an independent lab as a fallback option where no other wholly independent alternative is available.

Penalties for non-compliance must significantly exceed the profits obtained during the period(s) of non-compliance in order to serve as effective deterrents. These incentives may look different for each entity (the companies displaying the label,[21] the CLAs, and the Lead Administrator[22]), but the principle applies to all three. We have suggested several methods by which the Bureau might engage the Commission and other regulators to enact such deterrents for companies seeking to display the label.[23] For CLAs and for the Lead Administrator, the Bureau should seek to impose financial penalties for failing to fulfill their linchpin roles in a program

[15] For example, products that have been subject to substantiated complaints or to post-market surveillance indicating that the product did not merit the Trust Mark. We discuss complaints in our initial coalition comments. *See* Comments of Consumer Reports et al. at 1-2.
[16] *See* Reply Comments of Electronic Privacy Information Center (EPIC), PSHSB 23-239, at 27 (Nov. 10, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/111054758013.
[17] *See* R&O at ¶ 128 ("We believe it is appropriate for the Lead Administrator, in collaboration with the CLAs and other stakeholders, to identify or develop, and recommend to the Commission for approval, the post market surveillance activities and procedures that CLAs will use for performing post-market surveillance.").
[18] *See, e.g.*, Reply Comments of EPIC at 30 (Nov. 10, 2023).
[19] *See* RFC at ¶ 37, *available at* https://www.federalregister.gov/d/2024-14148/p-60 (noting that an in-house lab can serve as a CLA).
[20] Unless there are adequate internal controls to guard against such conflicts of interest, as many commenters have identified. *See* note 12 *supra*.
[21] *See, e.g.*, RFC at ¶ 16, *available at* https://www.federalregister.gov/d/2024-15379/p-45.
[22] *See, e.g.*, RFC at ¶ 14, *available at* https://www.federalregister.gov/d/2024-15379/p-43.
[23] *See, e.g.*, Reply Comments of EPIC at 33 (Nov. 10, 2023); Comments of Consumer Reports et al. at 2.

premised on consumer trust, in addition to the Bureau's existing authority to revoke their authorization for just cause.

IV. Conclusion.

We appreciate the Bureau's efforts to improve the cybersecurity of consumer products, and urge the Bureau to focus on preventing harm to consumers through the Bureau's attention to transparency, oversight, and accountability in its voluntary Trust Mark program.

Respectfully submitted, September 3, 2024.

Chris Frascella
Counsel
frascella@epic.org
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, D.C. 20036