Before the
Federal Communications Commission
Washington, DC

In the Matter of	)	
	)	
Cybersecurity Labeling for Internet of Things	)	PS Docket No. 23-239
	)	

REPLY COMMENTS OF CTIA

Umair Javed
Senior Vice President and General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

David Valdez
Vice President, Privacy and Cybersecurity

John A. Marinho
Vice President, Technology and Cybersecurity

Justin Perkins
Director, Cybersecurity and Policy

Mike Beirne
Director, Regulatory Affairs

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

September 3, 2024

TABLE OF CONTENTS

I. INTRODUCTION.. 1

II. TO HELP ENSURE SUCCESS, IT IS CRITICAL TO SECURE FEDERAL FUNDING SUPPORT RATHER THAN EXPECTING CLAS TO RECOVER PROGRAM COSTS THROUGH APPLICATIONS................................ 3

III. IN DEVELOPING THE IOT REGISTRY, THE FCC SHOULD PRIORITIZE MINIMIZING BURDENS. 7

A. CLAs Should Not Be Responsible for Managing or Updating the IoT Registry. 7

B. FISMA Should Not Apply to CLAs. 9

IV. CLA SELECTION CRITERIA NEED NOT INCLUDE ISO/IEC 17065 ACCREDITATION, BUT IF THE COMMISSION RETAINS THE REQUIREMENT, IT SHOULD EXTEND THE GRACE PERIOD FOR OBTAINING ISO/IEC ACCREDITATION. 9

V. THE COMMISSION SHOULD REJECT CALLS TO MANDATE DISCLOSURE OF INFORMATION THAT IS OUT OF SCOPE AND WILL DETRACT FROM THE PROGRAM'S FOCUS ON CYBERSECURITY...............11

VI. CONCLUSION 15

I. INTRODUCTION

CTIA is pleased to submit reply comments on the Public Notice ("Notice") on Implementation of the Cybersecurity Labeling For Internet of Things ("IoT") Program.[1] CTIA has consistently participated in this proceeding, including commenting on the Notice[2] and the August 2023 Notice of Proposed Rulemaking ("NPRM").[3] Launching this program is a substantial and complex undertaking, and that complexity can generate uncertainty for potential participants.[4] To encourage early adoption by a broad set of stakeholders, the Federal Communications Commission ("FCC" or "Commission") should reduce uncertainty and costs facing potential participants at all levels.

The record reflects consensus on one element that is critical for the program to succeed: securing federal funding to cover expenses related to consumer education.[5] However, there are

[1] Public Notice, 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 (rel. June 27, 2024) ("Notice").

[2] Comments of CTIA, PS Docket No. 23-239 (filed Aug. 19, 2024), https://www.fcc.gov/ecfs/document/10819238529940/1 ("CTIA PN Comments").

[3] Comments of CTIA, PS Docket No. 23-239 (filed Oct. 6, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10061240505270; Reply Comments of CTIA, PS Docket No. 23-239 (filed Nov. 10, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/111093246368.

[4] *See* Notice at ¶1, n. 3 (discussing "outstanding implementation issues in connection with the IoT Labeling Program" and previewing additional forthcoming Public Notices).

[5] *See e.g.*, Comments of NCTA – The Internet & Television Association, PS Docket 23-239, at 10 (filed Aug. 19, 2024), https://www.fcc.gov/ecfs/document/10819301318524/1 ("it is essential to deploy a Federal government-led initiative focused on consumer education") ("NCTA Comments"); Comments of Consumer Technology Association, PS Docket 23-239, at 15 (filed Aug. 19, 2024), https://www.fcc.gov/ecfs/document/10819119488751/1 ("broad consumer education should primarily be the responsibility of the federal government") ("CTA Comments").

other aspects of the program that would benefit from further consideration and clarification. To help ensure the program succeeds, the Public Safety and Homeland Security Bureau ("Bureau") should provide more predictability and limit obligations for potential Cybersecurity Label Administrator ("CLA") applicants and manufacturers that may seek to use the Cyber Trust Mark ("Mark").

In particular, the Bureau should reduce uncertainty about the role of CLAs and minimize the burdens that will be placed on CLAs. CLAs will not be able to successfully structure their certification programs without clear, concrete expectations about their obligations, including but not limited to the costs they will have to bear (and pass through to applicants). The nature of these costs and obligations should be defined in advance and should not be subject to significant change or revision after a CLA is approved. At a minimum, costs should be defined far enough in advance to allow prices for certification to be set reasonably.

The Bureau should also avoid creating unnecessary obligations for prospective CLAs that could promote inefficiencies and restrict participation. In particular, the FCC should not require ISO/IEC accreditation for those CLA applicants that have significant experience functioning in a similar role.[6] To the extent the Bureau does adopt a requirement for ISO/IEC 17065 accreditation, it should adopt an extended 18-month grace period for CLA applicants to obtain ISO/IEC accreditation following conditional approval. The six-month grace period contemplated in the March 2024 Order ("Order")[7] fails to account for the time typically necessary to obtain ISO/IEC accreditation, which includes time for the certifying organization to process the

[6] *See* Notice ¶ 6.

[7] *Cybersecurity Labeling for Internet of Things*, PS Docket No. 23-239, Report and Order and Further Notice of Proposed Rulemaking, FCC 24-26 (rel. Mar. 15, 2024) ("Order").

application. Restricting the grace period to six months will increase business uncertainty, as CLA candidates may be reluctant to undertake the significant investments necessary to participate in the program if their ability to issue approvals could be suspended after six months just because the accreditation body has not finished its work.

Nor should CLAs have a substantial role in maintaining the IoT registry; this would be an unnecessary complication that would increase CLA costs, which would in turn increase the cost of certification. Importantly, the Commission should also resist calls to dilute the focus of the program by seeking to address various privacy considerations. This would introduce undue complications and confusion, distract from the program's focus on cybersecurity, and unnecessarily duplicate existing disclosures related to privacy.

CTIA offers these recommendations to help the Commission successfully launch a viable program that can scale in the future.

II. TO HELP ENSURE SUCCESS, IT IS CRITICAL TO SECURE FEDERAL FUNDING SUPPORT RATHER THAN EXPECTING CLAS TO RECOVER PROGRAM COSTS THROUGH APPLICATIONS.

The record makes clear that establishing the program will require a substantial outlay of resources in a range of areas, including consumer education and developing program infrastructure. As CTIA noted in its comments, the "Order does not address how the Lead Administrator may be empowered or expected to fund consumer education efforts."[8] Numerous commenters agree that there is a need for federal funding for core aspects of the program like consumer education about the Mark,[9] which will be critical to the program's success.

[8] CTIA PN Comments at 4.

[9] *Id*. at 3. *See also* CTA Comments at 15; NCTA Comments at 10.

Commenters suggest that these costs should not be borne by the Lead Administrator or recovered via the CLAs from program applicants, as this would raise costs and discourage participation.[10]

Similarly, the Commission and Bureau should not expect that the Lead Administrator will pass a laundry list of costs through to CLAs and should reject calls by some for unpredictable cost-sharing by CLAs.[11] Fees will need to be predictable and CLAs must be capable of covering costs. Because CLAs will need to recover their own operational costs through fees charged to those seeking to use the Cyber Trust Mark, CLAs must be able to assess the costs of participating with sufficient certainty to be able to set fees for applicants. CLAs' costs will be especially difficult to recover at the outset of the program's operations when the program will presumably have the fewest applicants to use the new Cyber Trust Mark. Initial uptake of the program may depend on accessibility and charging modest fees to encourage voluntary use by manufacturers. Requiring CLAs to *also* recover substantial start-up costs for the broader program could drive overall CLA fees even higher, discouraging initial participation in the program and potentially leading to a vicious cycle where fee amounts spiral. This could discourage participation before the program can become established. CTIA strongly encourages the FCC to work with other government stakeholders to ensure federal funding support for the program and refrain from requiring CLAs to fund substantial costs to build, operate, and oversee the program, including for consumer education efforts.

[10] NCTA Comments at 5 ("The Federal government can help reduce these burdens on the Lead Administrator and CLAs by leading a consumer education campaign that increases the value proposition of Program participation.")

[11] *See* Comments of ioXt Alliance, at 4 (filed July 25, 2024), https://www.fcc.gov/ecfs/document/10725288307854/1 (suggesting that the Commission or some other "neutral oversight committee" determine fees that the Lead Administrator could charge CLAs).

CTIA and other commenters urged the Bureau and Commission to look to the Energy Star program as a model,[12] because it was sponsored by the Environmental Protection Agency ("EPA") and the Department of Energy ("DOE") with federal funding.[13] Of course, Congressional authorization may be required to secure adequate federal funding. To the extent it is necessary CTIA and others support seeking federal funding from Congress. But other sources of federal funding are also available, such as from the Department of Homeland Security Cybersecurity and Infrastructure Security Agency ("CISA").[14] Using these resources to fund the program would likely lead to quicker and more successful program rollout and implementation.

To keep CLA fees manageable, the FCC should also refrain from adopting the Wi-Fi Alliance's proposal, which suggests that "the Lead Administrator's expenses incurred in the performance of its duties should be shared proportionally among CLAs" and that "proportionality can be based on the number of products a CLA labels in a particular year."[15] Such an approach would be confusing and unpredictable and may discourage participation in the program. It will be impossible for CLA applicants to predict the cost structure in advance because the costs themselves are unknown and the Lead Administrator's "expenses will likely

[12] CTIA PN Comments at 5 ("The Energy Star program provides a good example of how federal funding can ensure an effective program with strong industry uptake."). *See also* Reply Comments of the Information Technology Industry Council, PS Docket No. 23-239, at 8 (filed Nov. 9, 2023), https://www.fcc.gov/ecfs/document/110978660645/1 (encouraging the Commission to manage the product registry, consistent with the Energy Star program model).

[13] *See, e.g.*, 10 C.F.R. pt. 430; 42 U.S.C. §§ 6291-6309.

[14] CISA, "*Secure Our World*," https://www.cisa.gov/secure-our-world (last visited Aug. 29, 2024).

[15] Comments of Wi-Fi Alliance, PS Docket No. 23-239, at 4 (filed Aug. 19, 2024) ("Wi-Fi Alliance Comments").

change over time."[16] So, if CLAs are expected to recoup their costs through fees for certifications, imposing the burden of sharing Lead Administrator costs would force prospective CLAs to take a cautious approach to recovering costs by setting higher initial fees, which could discourage manufacturers from seeking certifications.[17]

Indeed, the costs that the CLA faces may vary over time and fees must be adequate to recover their costs. CLAs may need flexibility to set varied fees depending on the type of applicant, the number of products at issue, and any other services they offer as part of the certification. Other organizations that license and oversee marks and certifications charge various and variable fees that they set in advance. For example, UL Solutions ("UL") charges an annual fee that "covers maintenance of client data and administrative fees related to your UL service" and a UL Mark Certification Fee for "use of the UL Mark 365 days a year (maintaining your ongoing certification)."[18] Energy Star participants have testing done by various third party certification bodies, who charge variable fees.[19] Given the uncertainties facing the launch of this

[16] *Id.* at 5.

[17] Comments of Infineon Technologies Americas Corp., PS Docket 23-239, at 2 (filed Aug. 19, 2024).

[18] UL Solutions, *UL Mark Certification Service FAQs*, https://www.ul.com/resources/ul-mark-certification-service-faqs (last visited Aug. 29, 2024).

[19] EPA Energy Star, "Certifying Products," https://www.energystar.gov/partner_resources/products_partner_resources/brand-owner/certifying-products (last visited Aug. 29, 2024) ("The cost and duration of product testing and certification varies by product category and [certification body.]"). *See also* EPA Energy Star, "What is the cost of third-party certification for ENERGY STAR?" (Sept. 15, 2020) https://energystar.my.site.com/ENERGYSTAR/s/article/What-is-the-cost-of-third-party-certification-for-ENERGY-STAR-1600088478191 (describing three approaches to Energy Star certification body certification costs: per-model charges, per-model charges with annual administrative fees, and one set annual fee per product category); Intertek, "ENERGY STAR®: General Questions," https://www.intertek.com/energystar/qanda/general-questions/, (last visited

voluntary program and the need to encourage uptake by manufacturers, costs imposed by the Lead Administrator should be established in advance and be predictable, and should not be subject to change after CLAs have set up their programs and fees.

III. IN DEVELOPING THE IOT REGISTRY, THE FCC SHOULD PRIORITIZE MINIMIZING BURDENS.

A. CLAs Should Not Be Responsible for Managing or Updating the IoT Registry.

To promote ready consumer access to information about approved products, the Order envisions maintaining a single registry of products that have received approval to use the FCC IoT Label.[20] In setting up the registry, the FCC stated in the Order that it will "require information about how to operate the device securely,"[21] but decided that a "modest," "decentralized, API-driven registry," would best serve consumer needs and leave open options for expansion.[22]

CTIA supports increasing consumer access to information.[23] But implementing the registry is potentially complex, especially if the roles and responsibilities of the various stakeholders are not clearly defined. In its comments, CTIA urged the Commission to ensure

Aug. 29, 2024) ("Intertek charges $2,500 per manufacturing location."); Bay Area Compliance Laboratories Corp., ENERGY STAR Product Certification User Manual, at 3 (Oct. 22, 2018), available at http://www.baclcorp.com/wp-content/uploads/QAM-UM-ESPC-B-ENERGY-STAR-Product-Certification-User-Manual.pdf ("All applicants are charged the same fee proportional to the scope of work, regardless of the number of certificates issued.")

[20] Order ¶ 111.

[21] *Id.* ¶ 115.

[22] *Id.* ¶ 116 ("[T]he decentralized, API-driven registry we adopt today addresses the complexity concerns raised in the record. We cabin our initial vision of the registry and direct the Bureau, as described further below, to consider ways to make the initial design of the registry modest, with potential to scale the registry as the IoT Labeling Program grows.").

[23] CTIA PN Comments at 3.

that the burdens associated with the registry are clear and limited, especially with respect to CLAs.[24] The Bureau should clarify the limited role of CLAs with respect to the creation, population, and maintenance of the registry and make clear that CLAs will not be responsible for or expected to bear possible additional costs that may be involved in developing and maintaining the registry, either initially or as the program develops. In its comments, CTIA urged the Bureau to clarify that CLAs will not be responsible for bearing the costs of building and maintaining the registry.[25] Several commenters agree.[26]

By contrast, the FCC should reject calls, like those from the TIC Council, that CLAs, rather than manufacturers, are the appropriate entities to "be responsible for the implementation and maintenance of the API" and to "update registry data in compliance with FCC requirements."[27] Such an arrangement will drive up costs for CLAs and will create substantial uncertainty that may make it difficult for CLAs to project costs and set fees.

[24] *Id*. at 10.

[25] *Ibid.* ("[A] CLA's role should be minimal compared to the Lead Administrator and manufacturers….")

[26] Wi-Fi Alliance Comments at 9 ("Manufacturers should be responsible for ensuring that the registry contains up-to-date information about their products"); Comments of Consumer Reports, et. al., PS Docket No. 23-239, at 5-6 (filed Aug. 19, 2024), https://www.fcc.gov/ecfs/document/10819759410275/1 (discussing proposed requirements for manufacturers to provide information to the registry) ("Consumer Reports Comments"); Comments of Information Technology Industry Council, PS Docket No. 23-239, at 4 (filed Aug. 19, 2024), https://www.fcc.gov/ecfs/document/108190403816504/1 ("manufacturers should be responsible for maintaining their own product data [and] should host the data") ("ITI Comments").

[27] Comments of TIC Council Americas, PS Docket No. 23-239, at 4 (filed Aug. 18, 2024), https://www.fcc.gov/ecfs/document/1081976943825/1. *See also* Comments of UL Solutions, PS Docket No. 23-239, at 7 (filed Aug. 19, 2024), https://www.fcc.gov/ecfs/document/10819106738061/1 ("UL Solutions Comments").

B. FISMA Should Not Apply to CLAs.

CTIA urged the Bureau to avoid imposing Federal Information Security Modernization Act (FISMA) obligations on contributors to the registry, since imposing such obligations may discourage participation.[28] The record demonstrates agreement that FISMA should not apply to CLAs, with commenters noting that the standards developed for government and government contractors under FISMA were not designed for non-governmental use and are not appropriate for private parties like CLAs.[29] FISMA compliance is costly and would impose burdens that would have to be passed through to manufacturers and drive up the cost of the program. Moreover, FISMA compliance could lead to delays in implementing the program. As the Consumer Technology Association explains, 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."[30] If compliance with FISMA or an equivalent regime were required, implementation of the Mark program would be on hold while potential participants sought appropriate certifications or took other steps to implement required security and privacy controls.

IV. CLA SELECTION CRITERIA NEED NOT INCLUDE ISO/IEC 17065 ACCREDITATION, BUT IF THE COMMISSION RETAINS THE REQUIREMENT, IT SHOULD EXTEND THE GRACE PERIOD FOR OBTAINING ISO/IEC ACCREDITATION.

In its comments, CTIA argued that to help ensure the success of the Cyber IoT Labeling program and avoid implementation delays, the FCC should prioritize organizations with a proven

[28] CTIA PN Comments at 10.

[29] CTA Comments at 10; UL Solutions Comments at 6; CTIA PN comments at 10.

[30] CTA Comments at 10.

track record administering certification programs when selecting CLAs.[31] CTIA also urged the Commission to adopt a flexible approach for any ISO/IEC accreditation requirement.[32] CTIA believes that the ISO/IEC accreditation requirement should be optional for entities with at least five to ten years of experience administering certification programs. Requiring all CLA candidates to go through the ISO/IEC 17065 accreditation process would increase costs and introduce new burdens without corresponding benefit. ISO accreditation is appropriate for CyberLabs but is not needed for experienced organizations that have managed cyber certification programs and that have experience in evaluating test lab activities.

To the extent the Bureau believes ISO/IEC 17065 accreditation remains necessary for all CLAs, CTIA urges the Bureau to adopt an extended 18-month grace period to obtain ISO/IEC accreditation for CLA applicants with at least five to ten years of experience administering certification programs. The six-month grace period contemplated in the Order[33] fails to account for the time typically necessary to obtain ISO/IEC accreditation, which includes the time necessary for the accreditation body to process and grant the application. These time periods are largely out of the applicant's control because they depend entirely on the processes of the accreditation body. A grace period that expires before certification can be granted would substantially disrupt business operations, making it difficult to plan. This risks artificially depressing the number of credible CLA applicants.

[31] CTIA PN Comments at 2.

[32] *Ibid*.

[33] Order ¶ 59.

V. THE COMMISSION SHOULD REJECT CALLS TO MANDATE DISCLOSURE OF INFORMATION THAT IS OUT OF SCOPE AND WILL DETRACT FROM THE PROGRAM'S FOCUS ON CYBERSECURITY.

The Cyber Trust Mark is correctly focused on cybersecurity, leveraging standards developed by the National Institute of Standards and Technology ("NIST") in close consultation with experts and industry over years. NISTIR 8425 serves as the core of the program and should remain the touchstone of the Mark program criteria.[34]

The FCC should resist calls by some in the record to add new obligations and guard against scope creep that would threaten to make the program unwieldy. Some commenters urged the FCC to dilute the focus of the registry by mandating the inclusion of information unrelated to cybersecurity. The Future of Privacy Forum ("FPF"), for example, calls for the adoption of additional information disclosure mandates unrelated to the device's cybersecurity profile, suggesting that "[i]nformation about devices' sensors and data practices can help people make better decisions…."[35] In discussing privacy issues potentially raised by some IoT devices, FPF contends that "[t]he aggregation of personal data may allow those collecting it to learn or infer sensitive information about people, or to track people's behaviors across different spaces."[36] Similarly, Consumer Reports advocates extending the program to address "more than the original 10 elements required by the Report and Order" by adding multiple privacy-focused issues.[37] Consumer Reports' comments identify many additional elements that it wants to see in the

[34] Order at ¶ 9 ("NIST's essential work . . . provide[s] the building blocks for our development and adoption of this IoT Labeling Program.").

[35] Comments of Future Privacy Forum, PS Docket No. 23-239, at 2 (filed Aug. 19, 2024), https://www.fcc.gov/ecfs/document/10819207705990/1 ("FPF Comments").

[36] *Ibid*. (footnote omitted).

[37] Consumer Reports Comments at 2.

mandated contents of a registry and product disclosures, including several categories that reflect value and policy judgments that are far afield from NISTIR 8425.[38] These proposals would be burdensome and provide information that is of unclear or dubious value to the average consumer, as described below.

Significantly expanding the Mark program's requirements to require disclosure of privacy-related information at this stage threatens to derail the program by increasing complexity and confusing consumers.[39] The Commission should not require the registry, for example "to list the sensors contained in the complying product, such as cameras, microphones, and location tracking devices" or "what data is collected by those sensors, and whether that data is shared with third parties."[40] Nor should it impose new requirements on participants to include specific information about vulnerability disclosure programs and processes.[41]

First, voluminous information about varied topics, as proposed, is likely to confuse rather than inform consumers, by overloading them with information that is not relevant to the specific issue of cybersecurity.[42] The type of information that should populate the registry should be

[38] *Id*. at 3 (suggesting that the mandatory consumer facing disclosures should identify the entities that the sensor data is shared with, using a particular Carnegie Mellon schema, among other proposals).

[39] NCTA Comments at 10 (Information collection disclosure mandates "address distinct privacy concerns separately covered by various state and federal laws and thus fall outside the Program's scope."); WiFi Alliance Comments at 9 ("[T]here is a risk that consumers will find such disclosures more overwhelming than helpful."); ITI Comments at 3; CTIA PN Comments at 11.

[40] Notice ¶ 21.

[41] Consumer Reports Comments at 3.

[42] *See* ITI Comments at 2; Comments of Association of Home Appliance Manufacturers, PS Docket No. 23-239, at 2 (filed Aug. 16, 2024) ("AHAM Comments"); NCTA Comments at 10 ("[D]etailed disclosure mandates concerning what information the manufacturer is collecting,

tailored, minimal, and designed to educate consumers about security, not overwhelm them with additional information about other issues. The complexity and diversity of products and the potential for consumer confusion counsel in favor of a modest approach to the information that is required in the registry. Expanding the registry's scope to include detailed privacy-related data and disclosures runs the risk of turning it into a catch-all set of disclosures, which would dilute the effectiveness of the cybersecurity messaging. Introducing additional complexity and confusion to the label is also unnecessary because manufacturers and other stakeholders routinely include information about privacy practices, data use, and other information in their privacy policies and other materials.[43] The privacy proposals put forward in the record are complex and require policy analysis and decision-making that is entirely separate from the targeted cybersecurity mandate embodied in the Order.[44]

Second, the information conveyed by the label should be as consistent across products as possible, to facilitate the kind of comparison shopping contemplated by the Trust Mark program. If privacy information is added to the label or registry, it could make such straightforward comparisons on cybersecurity issues more difficult.[45] Consumers will not easily be able to

and how it is being used or shared, address distinct privacy concerns separately covered by various state and federal laws and thus fall outside the Program's scope.").

[43] CTA Comments at 13 ("Manufacturer disclosures should avoid either overwhelming consumers with too much information or duplicating information often disclosed elsewhere where a consumer already knows to look (such as a privacy policy).").

[44] *See* Caven et. al., *Comparing the Use and Usefulness of Four IoT Security Labels*, CHI '24: Proceedings of the CHI Conference on Human Factors in Computing Systems, Honolulu, HI, May 2024 (2024), https://dl.acm.org/doi/fullHtml/10.1145/3613904.3642951 (discussing the challenges of implementing a "Privacy Nutrition Label"—"[s]ome users found the labels to be helpful; though most found them to still be too long, complex, or confusing").

[45] Wi-Fi Alliance Comments at 9 ("[b]ecause of the diversity and unique features of IoT products, it is impractical for the Commission to mandate specific product disclosure requirements.").

understand why this information is being disclosed in a cybersecurity registry, or how the information should impact their assessment of the cybersecurity of the device.

Third, providing detailed information on data collection could create security and confidentiality risks by providing malicious actors with a roadmap to information they could leverage.[46] Detailing exactly which sensors collect certain types of data would allow a potential attacker to select publicly known vulnerabilities to target particular information used by a device.[47] Mandatory disclosures that directly tie specific sensors to specific data could also compromise proprietary information and trade secrets.[48]

Fourth, because consistently protecting the confidentiality of sensitive information will encourage manufacturer and CLA participation, the Bureau is correct to conclude that manufacturer and CLA applications should be treated as presumptively confidential.[49] While one commenter does seek disclosure of manufacturer applications in order to review test methodologies,[50] the majority of commenters support treating applications as confidential[51]—and the test methodologies will likely be public in any event.

[46] *See* ITI Comments at 3. *See also* Reply Comments of Garmin International, Inc., PS Docket No. 23-239, at 2 (filed Nov. 13, 2023), https://www.fcc.gov/ecfs/document/1113243476430/1 ("participating manufacturers should not be required to provide public notice on the Registry of any matters that would potentially jeopardize device security")(alteration omitted).

[47] ITI Comments at 2-3.

[48] *Ibid*.

[49] Notice at ¶17.

[50] Comments of Consumer Reports, et. al., PS Docket No. 23-239, at 2 (filed Aug. 19, 2024), https://www.fcc.gov/ecfs/document/10819759410275/1.

[51] *See* Comments of American Association for Laboratory Accreditation, at 3 (filed Aug. 19, 2024) https://www.fcc.gov/ecfs/document/1081999874923/1 ("We cannot think of any reason why CLA or LA applications, or their contents, should be made known to the public."). *See also* NCTA Comments at 2 ("NCTA supports the Bureau's determination that manufacturer applications submitted to Cybersecurity Label Administrators…be treated as presumptively

Because of the host of concerns raised by proposals to incorporate significant privacy disclosures, the Bureau and Commission should keep the program and registry focused on cybersecurity, as it has been structured since the White House's announcement. This focus should remain on the use of the NISTIR 8425 "Product Education and Awareness" criteria as the baseline for the Mark label,[52] and resist calls to expand the program to provide additional disclosures beyond what is relevant to obtaining authorization to use the Mark.[53] The data included in the registry should remain focused on security issues directly relevant to the Mark and should not add information that may be relevant to other policy objectives. There is a substantial risk of consumer confusion if the registry includes information that does not bear on whether the product qualifies for the Mark.

VI. CONCLUSION

In moving to operationalize the program, CTIA encourages the Commission to take steps to ensure that proposed obligations on potential participants do not dissuade key stakeholders from supporting the Mark. To ensure that a broad group of market participants join the program, the FCC should seek federal funding for promoting the Mark and promote transparency and predictability in CLA costs by keeping obligations for maintaining and updating the registry narrow. The FCC should also not require potential CLAs to obtain unnecessary certifications. The Commission should reject proposals to expand the scope of the data provided to the registry.

confidential and be protected by reasonable information security measures."); CTA comments at 14 ("failing to provide confidential treatment of these in-process documents would serve little-to-no public interest, because the label itself discloses important product information").

[52] NISTIR 8425., Profile of the IoT Core Baseline for Consumer IoT Products, NIST Internal Report, NIST at 16 (Sept. 2022), https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.pdf, ("NISTIR 8425").

[53] CTA Comments at 12; AHAM Comments at 2.

CTIA welcomes engagement with the Commission on next steps to implement the Mark program.

/s/ David Valdez
David Valdez
Vice President, Privacy and Cybersecurity

Umair Javed
Senior Vice President and General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Justin Perkins
Director, Cybersecurity and Policy

Mike Beirne
Director, Regulatory Affairs

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200