Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

REPLY COMMENTS OF CONSUMER TECHNOLOGY ASSOCIATION

J. David Grossman
Vice President, Regulatory Affairs

Mike Bergman
Vice President, Technology & Standards

Rachel S. Nemeth
Senior Director, Regulatory Affairs

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7651

November 13, 2023

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

REPLY COMMENTS OF
CONSUMER TECHNOLOGY ASSOCIATION

Consumer Technology Association (CTA)®[1] respectfully submits these reply comments in response to the Federal Communications Commission's ("Commission's" or "FCC's") Notice of Proposed Rulemaking (*NPRM*) on *Cybersecurity Labeling for Internet of Things*.[2]

I. INTRODUCTION AND SUMMARY

The record overwhelmingly demonstrates strong support from manufacturers, retailers, public interest groups, and industry, including CTA and its members, for the Commission's proposal to establish the U.S. Cyber Trust Mark (Mark) Program (the Program) as a voluntary program based on the multi-year effort between the National Institute of Standards and Technology (NIST) and stakeholders to develop baseline security capabilities for Internet of Things (IoT) devices and the profile for consumer IoT cybersecurity labeling. Indeed, CTA joined eleven fellow trade associations in a recent letter expressing support for the Program, noting appreciation for the Commission's collaboration in this effort and outlining eight

[1] As North America's largest technology trade association, CTA® is the tech sector. Our members are the world's leading innovators—from startups to global brands—helping support more than 18 million American jobs. CTA owns and produces CES®—the most powerful tech event in the world.

[2] *Cybersecurity Labeling for Internet of Things*, Notice of Proposed Rulemaking, FCC 23-239 (rel. Aug. 10, 2023) (*NPRM*). Consistent with Rule 1.4, CTA is filing these comments on November 13, 2023. *See* 47 CFR § 1.4(j) (providing that if a filing date falls on a holiday, the document must be filed on the next business day). The federal government observed Veterans Day on November 10, 2023.

In these reply comments, all comments filed on or about October 6, 2023, in this proceeding are short cited by name of party.

principles on which stakeholders broadly agree that the Program should be founded.[3] This public-private partnership effort has great potential to reduce systemic cybersecurity risk to internet infrastructure and users of connected devices.

The task now falls to the Commission to establish this Program to support efficient procedures for use of the Mark, apply rules consistently and equitably across program participants, and enable the Program to evolve over time. To achieve these goals, the Program must embrace opportunities to minimize administrative burdens and other participation costs while promoting public trust in the Mark. In particular, the Commission must establish a process for self-attestation, streamline the review and renewal process for devices bearing the Mark, and leverage modern industry practices like e-labeling and other technology solutions. Ultimately, as commenters widely recognize, implementing the U.S. Cyber Trust Mark must be an iterative process that allows the Commission and stakeholders to modify and expand the Program with the benefit of experience over time.

We elaborate on these points below and look forward to continued collaboration with the Commission to implement and grow the Program.

II. STAKEHOLDERS SUPPORT THE COMMISSION'S PROPOSAL TO ESTABLISH A VOLUNTARY LABELING PROGRAM BASED ON THE NIST CRITERIA

Commenters—including CTA and its members who represent a wide variety of large and small device manufacturers, retailers, systems integrators and more—support the Commission's proposal to establish the Program based on the multi-year effort between NIST and stakeholders

[3] Letter from Association of Home Appliance Manufacturers (AHAM), Connectivity Standards Alliance (CSA), Consumer Technology Association (CTA), CTIA, Information Technology Industry Council (ITI), National Electrical Manufacturers Association (NEMA), Plumbing Manufacturers International, Power Tool Institute, Security Industry Association (SIA), Telecommunications Industry Association (TIA), U.S. Chamber of Commerce, and USTelecom, to Marlene H. Dortch, Secretary, Federal Communications Commission, PS Docket No. 23-239 (filed Nov. 8, 2023).

to develop baseline security capabilities for IoT devices in the NISTIR 8259 Series and Consumer IoT Profile directed by Executive Order 14028. At a high level, commenters agree that:

- The Program's top-line goal should be to reduce systemic cybersecurity risk to internet infrastructure and users of connected devices.[4]
- The Program must be voluntary to ensure the broadest reach, most efficiency, and widest access to the diversity of IoT technologies.[5]
- Building the Program on a robust foundation of existing NIST guidance, industry standards, established third-party conformity assessment processes, and a streamlined self-attestation process aligned to existing NIST Criteria is important both for speed and for ultimate success.[6]
- The Commission must: incentivize robust manufacturer participation through liability protection; emphasize consumer education; promote international alignment; prioritize self-attestation; and safeguard trust in the Program's integrity through objective, transparent and rigorous processes.[7]
- Achieving this vision with speed and efficiency requires a whole-of-government effort across the U.S. government and close partnership with industry stakeholders and consumers.[8]

[4] *See, e.g.*, Comcast Corporation (Comcast) at 1; Consumer Reports at 2; CSA at iii; CTA at 5-7; CTIA – The Wireless Association (CTIA) at 1; Cybersecurity Coalition at 1; ITI at 2; Samsung Electronics America (Samsung) at 1; TechNet at 2.

[5] *See, e.g.*, AHAM at 2; CTA at 4; CTIA at 15; National Association of Manufacturers (NAM) at 2; NTCA – The Rural Broadband Association (NTCA) at 4; TIA at 2; USTelecom at 11-12; Widelity, Inc. (Widelity) at 1-4; Wi-Fi Alliance at 10.

[6] *See, e.g.*, AHAM at 4; Comcast at 11; Consumer Reports at 11; CTA at 11; CTIA at 16; Cybersecurity Coalition at 4; ioXt Alliance at 6; ITI at 7; Samsung at 3; UL Solutions at 4.

[7] *See, e.g.*, Comcast at 10; CSA at 20; CTA at 4; NCTA at 10-11; Samsung at 5-6. Among those incentives, commenters generally agree that the FCC should work with public and private sector partners to promote international harmonization and pursue mutual recognition with foreign IoT labeling regimes. *See, e.g.*, CTA at 30-31; CTIA at 42; Cybersecurity Coalition at 1-2; Garmin at 10-11; ITI at 6; Samsung at 6; Widelity at 4. Commenters also highlight the importance of education to spread awareness of the Program, with some offering suggestions on how to target messaging to meet distinct needs between consumers, Program participants, and other stakeholders. *See, e.g.,* Samsung at 4; USTelecom at 11.

[8] *See e.g.*, Consumer Reports at 11; UL at 4; AHAM at 6; Garmin at 17-18; ioXt at 25; NAM at 2; Comcast at 11; Infineon at 4; NCTA at 4; Samsung at 3-4.

III. THE PROGRAM STRUCTURE SHOULD SUPPORT EFFICIENT APPROVALS, UNIFORM APPLICATION OF THE RULES, AND DYNAMIC EVOLUTION OVER TIME

The Commission should establish clear roles and responsibilities that leverage the unique expertise and resources of each entity participating in the Program, as well as ensure uniform application of the rules. This will enable the Program to move forward with speed and efficiency while enabling its dynamic evolution to reflect technology and market developments. At a high level, the Commission should serve as the overarching Program Owner and approve "Authorized Scheme Owners" to develop and manage Schemes to implement the Program's rules. The Program requirements for achieving the Mark should be based on the NIST Consumer IoT Profile, and NIST should maintain primary responsibility for convening stakeholders to update that criteria and related guidance over time. The Commission should approve Third-Party Administrators to conduct Program operations and CyberLABs to conduct third-party testing and conformity assessment.

A. Commenters Explain that the Commission Should Serve as the Ultimate Program Owner and Leverage "Authorized Scheme Owners" for Implementation

The record reflects general agreement that the Commission should serve as the overall Program administrator (referred to in some comments as "Scheme Owner").[9] Establishing the Commission as the ultimate Program Owner will ensure clear and consistent application of the rules and avoid variation that could confuse consumers and limit the Program's effectiveness.[10] As the Cybersecurity Coalition notes, a single administrator reduces the likelihood of conflict

[9] *See, e.g.*, AHAM at 3; CTA at 16; Cybersecurity Coalition at 5; ioXt Alliance at 13; UL Solutions at 6.

[10] *See, e.g.*, TIC Council at 3-4; NIST Recommended Criteria at 2 (noting that "multiple variations of labels or labeling approaches would likely cause confusion among consumers and limit the effectiveness of the efforts.").

among administrators and simplifies engagement with manufacturers, consumers, and government agencies.[11] However, the FCC cannot and should not perform these functions alone. The Commission should leverage industry organizations to serve as "Authorized Scheme Owners" to develop pathways (or "Schemes") for approval to use the Mark under the Commission's rules. This may involve assessing a candidate Scheme against some framework of the NIST Criteria, such as draft ANSI/CTA-2119.[12]

If an Authorized Scheme Owner tests for conformity against the Scheme as a third-party conformity assessment body, then it should also meet accreditation requirements (for conformity assessment and for the domain) and other industry and international norms to issue the Mark under its Scheme and according to terms in a Mark license agreement. At a minimum, an Authorized Scheme Owner would maintain the Scheme, keep it up-to-date and respond to inquiries regarding the Scheme, and could perform conformity assessment against that Scheme.

A qualified manufacturer should be authorized to attest that their own product and processes comply with the NIST Criteria. To verify these qualifications in a uniform fashion, the Commission should also use a framework to assess manufacturer attestations against the NIST Criteria. More information on this process is presented in *Annex A: Scheme Evaluation Framework*.[13] In addition to a uniform Framework, the Commission should consider the value of automated testing that can evolve to fit the needs of the Program.

[11] Cybersecurity Coalition at 5.

[12] ANSI/CTA-2119, Framework for Evaluation of a Cybersecurity Scheme (draft, contact CTA for details).

[13] *See Annex A: Scheme Evaluation Framework*, *infra* A-2 (regarding draft ANSI/CTA-2119-A).

B. NIST's Consumer IoT Profile Should Inform the Program Criteria and NIST Should Update the Criteria as Needed Over Time

Commenters overwhelmingly agree that NIST should be the central repository for developing and maintaining the baseline cybersecurity capabilities and related IoT security guidance that form the foundation of the Program requirements.[14] NIST's established process for developing and maintaining this guidance through the Cybersecurity for IoT Program will provide a robust opportunity for stakeholders to flag updates for consideration and for subject matter experts to determine how these updates can be incorporated into the Criteria and technical requirements. This approach will also ensure that the Program evolves in harmony with related efforts across the federal government, such as sector specific guidance under development at the Department of Energy and rules for federal procurement of IoT.[15]

C. Third-Party Administrators Should Perform Program Operations and the Commission Should Approve CyberLABs for Participants Seeking Third-Party Conformity Assessment

The Commission should also leverage Third-Party Administrators and CyberLABs to help implement the Program. The record underscores that the FCC should authorize Third-Party Administrators to perform Program operations such as conformity assessment accreditation,

---

[14] *See, e.g.*, AHAM at 4; Comcast at 11; Consumer Reports at 11; CTA at 11; CTIA at 16; Cybersecurity Coalition at 4; ioXt Alliance at 6; ITI at 7; Samsung at 3; UL Solutions at 4.

[15] *See* Press Release, White House, Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers (July 18, 2023) (announcing DOE collaborative initiative with National Labs and industry partners to research and develop cybersecurity labeling requirements for smart meters and power inverters), https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/; NIST, NIST SP 800-213: *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*, https://csrc.nist.gov/pubs/sp/800/213/final (to be incorporated into the Federal Acquisition Regulations pursuant to the IoT Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207, § 4(d), 134 Stat. 1001, 1003 (2020)).

domain accreditation, conformity assessment testing, and sublicensing of the Mark.[16] Numerous commenters note that a Third-Party Administrator may also be better positioned to manage the IoT Registry.[17] The Commission should approve CyberLABs to assess IoT devices for compliance with IoT cybersecurity standards that meet Program requirements.[18] As discussed below, while some manufacturers will choose self-attestation—which is a separate matter and detailed in Annex C—many will opt for third-party conformity assessment to meet requirements in various jurisdictions or to satisfy customer demands.[19]

IV. THE PROGRAM SHOULD MINIMIZE ADMINISTRATIVE BURDENS AND COST TO PARTICIPATE WHILE MAINTAINING TRUST IN THE MARK

To run the Program efficiently and incentivize manufacturer participation, the Commission should embrace mechanisms that streamline administrative processes while maintaining the integrity of the Mark. Importantly, the Commission should establish a process for self-attestation to promote efficiency and scale of the Program. CTA views self-attestation as a key component of ensuring manufacturer participation and program success. The Commission should also ensure streamlined processes for reviewing device certification[20] where required, and renewing authorization when necessary. This includes keeping the Program distinct from Commission equipment authorization, allowing for model line approval, requiring renewal only when there has been a material change in the security posture of a device bearing the Mark, and aligning to internationally recognized processes for coordinated vulnerability disclosure. The

[16] *See, e.g.*, AHAM at 3; CSA at 5-6; CTA at 16-18; CTIA at 26-27; Cybersecurity Coalition at 5; ITI at 8; Widelity at 3.

[17] *See, e.g.*, ITI at 9-10; Widelity at 3.

[18] *See, e.g.*, AHAM at 3; CTA at 27-28; CTIA at 26; NCTA at 7; NAM at 3-4; UL at 2-3.

[19] *See Annex C: Regarding Trust Mechanisms*, *infra* A-11.

[20] "Certification" is a term of art in industry. While it is used in certain Commission processes, the more general usage is intended in this document.

Commission should also embrace other mechanisms for reducing cost and administrative burdens on the Program, such as allowing Program participants to use e-labels.

A. The Program Must Allow for Self-Attestation in Addition to Third Party Conformity Assessment

Commenters broadly agree that for the Program to operate efficiently and at scale the Commission must provide an option for self-attestation in addition to third-party conformity assessment of IoT devices.[21] Self-attestation will ease international harmonization with other countries and regions that have included self-assessment or self-attestation processes, such as the EU as part of the Cyber Resilience Act (CRA),[22] Germany through the Federal Office for Information Security (BSI),[23] or Singapore through the Cybersecurity Labeling Scheme.[24] As Samsung notes, relying only on third-party conformity assessment could result in delays to market and hinder U.S. innovation, along with adding unsustainable strain and expense to the Program's administration.[25] Self-attestation can help streamline this process, particularly as the Program grows. Moreover, as ITI recognizes, vendors and suppliers are often best positioned to identify the combination of standards that address their specific risk profiles and business

[21] *See, e.g.*, AHAM at 3; Consumer Reports at 20; CSA at 12; CTA at 18; CTIA at 26-27; Cybersecurity Coalition at 6; Garmin at 12; ioXt Alliance at 18; ITI at 6; LG at 2; NAM at 4; Samsung at 5; USTelecom at 6; Wi-Fi Alliance at 6.

[22] *See* European Commission, EU Cyber Resilience Act, Shaping Europe's Digital Future (last updated June 20, 2023), https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

[23] *See* Federal Office for Information Security, Questions and answers for customers for the IT Security Label, (last visited Nov. 9, 2023), https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/IT-SiK-fuer-Verbraucher/FAQ-IT-SiK-fuer-Verbraucher/faq_it-sik-verbraucher_node.html.

[24] *See* CSA Singapore, Cybersecurity Labelling Scheme (CLS), (last updated Nov. 9, 2023), https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme.

[25] Samsung at 5.

models.[26] Several commenters also observe that providing a path for self-assessment will allow manufacturers to better protect sensitive and confidential information about their products.[27]

Other commenters argue that self-assessment should be verified by FCC-approved Third-Party Administrators or CyberLABs during the application process.[28] Such verification simply moves the trust extended to the manufacturer to other points that are still under the manufacturer's control, since in self-attestation the manufacturer conducts the testing. Alternatively, Consumer Reports advocates that self-attestation may be allowed for certain low-risk devices, such as those that do not have associated apps or cloud connections.[29] However, distinguishing devices eligible for self-assessment based on risk level would overly complicate the process and require nuanced value judgements by the Commission that are likely to shift dynamically throughout the life of a device bearing the Mark and throughout the course of the Program.

These comments effectively propose to remove some level of the trust required of self-attestation. But because self-attestation is a first-party approach, there is no such option that removes risk entirely. Many manufacturers already meet the NIST Criteria and should be extended that trust through self-attestation. The process, however, should not require a third-party review or accreditation, as such steps add additional administrative burden and delay without changing the basic trust dynamics.

Instead, CTA proposes a self-attestation process that recognizes the nature of trust in self-attestation, as is appropriate with a first-party approach, and is rooted in NISTIR 8425. And even

[26] ITI at 8.

[27] *See, e.g.*, Garmin at 12; NAM at 4.

[28] *See* ioXt Alliance at 18; NAM at 4.

[29] Consumer Reports at 20.

with a self-attestation option, many Program participants may still choose third-party conformity assessment based on customer demand or to meet regulatory requirements in particular jurisdictions.[30] A detailed proposal for Manufacturer's self-attestation is presented in Annex C.[31]

B. The Commission Should Streamline Review and Renewal of Devices Bearing the Mark

1. TYING THE U.S. CYBER TRUST MARK PROGRAM TO EQUIPMENT AUTHORIZATION WILL BE COUNTERPRODUCTIVE

Commenters generally agree that completing Commission equipment authorization should not be a prerequisite of achieving the Mark.[32] Requiring these separate programs to be run serially will introduce needless delay into product development cycles and generate consumer confusion as some devices enter the market the same day as equipment authorization.[33] CSA suggests that although the Commission may find it prudent to keep the operation of the Program separate and distinct from equipment authorization, there should be systemic coordination between the two to consider any potential delays in the approval process.[34] However, provided that the Commission keeps these processes distinct, we do not see a situation in which such coordination would be necessary. The Program and equipment authorization processes should remain distinct from each other.

---

[30] For example, California's IoT law requires "conformity assessment as described by a NIST conforming labeling scheme that includes a third-party test, inspection, or certification" to use the NIST Criteria to satisfy California's reasonableness requirement. Cal. Civ. Code § 1978.91.04(c)(2) (2023).

[31] *See Annex C: Regarding Trust Mechanisms*, *infra* A-11.

[32] *See, e.g.*, Consumer Reports at 35; CTA at 21-22; ITI at 4; TIA at 2.

[33] *See* CTA at 21-23.

[34] CSA at 19-20.

2. MODEL LINE APPROVALS WILL IMPROVE THE EFFICIENCY AND SCALE OF THE PROGRAM WITHOUT INTRODUCING RISK

To facilitate efficient approvals, whether through third-party conformity assessment or self-attestation, the Program should expressly permit "model line" assessments and approvals. As AHAM notes, the Program should allow manufacturers to register an IoT device that is used across multiple product models, without requiring a manufacturer to assess every individual model, and accept approval of the specific component and permit the Mark to be applied to each model using the component.[35] In practice, this would allow, for example, a smart TV model line from smaller screens up to the largest screen in that model group to achieve the Mark simultaneously and/or through a single qualification, provided that the underlying hardware and software are the same throughout the model line. Allowing model line approvals will help streamline the process and reduce administrative and participation costs without compromising any security assurance in the process.

3. THE PROGRAM SHOULD REQUIRE RENEWAL ONLY WHEN THERE HAS BEEN A MATERIAL CHANGE IN THE SECURITY POSTURE OF THE APPROVED DEVICE

The Program should require renewal based on material changes in the security posture of the device bearing the Mark rather than arbitrarily requiring annual renewal, which will raise the cost of Program participation and increase the administrative burden on the Commission. As AHAM notes, the requirement to renew an approval should only be triggered when there is a substantive change to the standard underlying the approval, a security breach that forces a change in the baseline requirements, or when there is a significant design change to the device, provided those changes are within the boundary and scope of the Program.[36] This is consistent

[35] AHAM at 6.

[36] *Id.* at 4.

with commenters like NAM who—despite suggesting that the Commission consider the risk profile of a device in determining whether to require a renewal—condition the need for renewal based on the discovery of critical vulnerabilities or significant updates to the product.[37]

4. PROGRAM PARTICIPANTS SHOULD FOLLOW INTERNATIONAL STANDARDS FOR COORDINATED VULNERABILITY DISCLOSURE

As many commenters in the record note, the Program should rely on internationally-recognized standards and best practices for coordinated vulnerability disclosure (CVD), such as ISO/IEC 30111 and ISO/IEC 29147, referred to in the IoT Cybersecurity Improvement Act, to establish expectations for Program participants to address vulnerabilities in devices that bear the Mark.[38] These programs provide manufacturers a reasonable period of time for remediation after a vulnerability is discovered, while managing communication about the vulnerability with stakeholders in a way that protects the ecosystem's security interests.[39] It also provides an objective and transparent standard for ensuring that Program participants adequately address vulnerabilities as they arise.[40]

C. The Program Should Leverage E-Labeling

Commenters broadly agree that the Program should leverage processes—like e-labeling—that can reduce burdens on the Program and its participants and help maintain the

[37] NAM at 5-6.

[38] *See, e.g.*, Consumer Reports at 30-31; Garmin at 19-20; ioXt Alliance at 22-23. *See also* IoT Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207, § 2, 134 Stat. 1001, 1004 (2020).

[39] *See* J. David Grossman & Mike Bergman, *Coordinated Disclosure of Cyber Vulnerabilities is a Win for Consumers and Industry*, CTA (2022), https://www.cta.tech/Resources/Articles/2022/Coordinated-Disclosure-of-Cyber-Vulnerabilities-is.

[40] *See* ioXt Alliance at 23 (noting, for example, that if a participant in their certification program fails to remediate a vulnerability through their vulnerability disclosure program, the product loses its certification and is delisted from the ioXt registry).

validity of communication to consumers over time.[41] As CTA noted in initial comments, manufacturers should have as much flexibility as possible in affixing the Mark to the packaging of products, including the location of the Mark or through e-labeling, so long as variation does not confuse consumers.[42] For example, a manufacturer may want to place the Mark (shield only) prominently on the front of a product package, with the Mark and QR code on the back for reference to the on-line information. Flexibility to use the Mark in such ways benefits the Program by encouraging manufacturer participation and raising awareness.

V. THE RECORD SHOWS THAT IMPLEMENTING THE U.S. CYBER TRUST MARK MUST BE AN ITERATIVE PROCESS

Stakeholders have yet to reach consensus on key questions including whether to focus the Program on IoT devices versus products and whether and how to establish a centralized IoT Registry. However, even stakeholders with differing views on these issues envision additional clarity emerging throughout the experience of administering the Program. They also recognize that aspects of the Program—such as the technical criteria and scope—will need to evolve over time. Numerous commenters call on the Commission to issue a Further Notice of Proposed Rulemaking to examine these elements.[43] The Commission may find it helpful to seek additional comment on specific aspects of the Program, such as proposed rule text and label design, as well as the structure and process for maintaining the IoT registry. CTA encourages the Commission to view establishment of the Program as an initial step and to build robust opportunities to continue collaborating with stakeholders as the Program is implemented.

[41] *See, e.g.*, CTA at 32-33; ITI at 9; Wi-Fi Alliance at 11.

[42] CTA at 32-33.

[43] *See, e.g.*, AHAM at 1.

VI. CONCLUSION

The record demonstrates widespread support for a voluntary U.S. Cyber Trust Mark program for consumer IoT, facilitated through public-private collaboration, that combines government criteria, industry consensus standards, and existing industry assessment and approval processes. The task ahead is to implement this Program in a way that can quickly and effectively initiate approvals, which can be achieved by leveraging existing infrastructure and taking an iterative approach. CTA looks forward to continuing to assist the Commission to stand up a successful U.S. Cyber Trust Mark Program.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

By: */s/ J. David Grossman*
J. David Grossman
Vice President, Regulatory Affairs

/s/ Mike Bergman
Mike Bergman
Vice President, Technology & Standards

/s/ Rachel S. Nemeth
Rachel S. Nemeth
Senior Director, Regulatory Affairs

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7651

November 13, 2023

ANNEXES

In these Annexes, CTA presents work-in-progress on American National Standard (ANS) documents that describe how to operationalize aspects of the U.S. Cyber Trust Mark (Mark) Program (the Program). As the Commission will own the Mark Program and determine the Program's rules, the Commission will ultimately decide whether to adopt such documents via "incorporation by reference" into Commission rules and/or guidance.

CTA presents these draft materials to show progress toward the following goals:

1. Define a Framework that is a standardized and objective method of applying the Criteria in NISTIR 8425 to a candidate Scheme or to a manufacturer's proposal for self-attestation for the Program.
2. Standardize program labeling requirements for the Mark, QR code and online information.
3. Define how to use available trust mechanisms such as self-attestation and third-party conformity assessment.

Representatives from more than thirty entities participate in the working groups, including staff from IoT manufacturers, chip makers, retailers, test houses, trade associations, standards bodies, industry alliances, and consumer advocates. NIST is also participating, assisting in understanding the intent behind elements of the Criteria.

CTA anticipates completing these documents in 2024, however, timing will depend on the Commission's need to review, publish, accept comments, or otherwise comply with the requirements associated with Program adoption. CTA recommends working jointly with the Commission to develop a timeline, should these proposed documents be given further consideration.

Annex A: Scheme Evaluation Framework

In this Annex, CTA presents draft material prepared by the Scheme Evaluation Framework working group of CTA's ANSI-accredited standards program; this working group is designated "R14 WG6" in the CTA program. This group is a subgroup of the Cybersecurity and Privacy Management Committee (designated "R14").

The group's work is progressing. The material here is presented as an example of the form and rigor of the finished document. The final document will be ANSI/CTA-2119, Scheme Evaluation Framework, and is anticipated to be completed during the first half of 2024.

To be clear, the Framework is not a Scheme. The Framework is a way to evaluate candidate Schemes against NISTIR 8425 in a transparent and objective fashion.

Framework Overview

The document purpose is described in its section 5, Background and Purpose:

> *The NIST publication NISTIR 8425, Profile of the IoT Core Baseline for Consumer IoT Products, provides technical and non-technical requirements, label requirements and conformity assessment requirements. Together, these documents are known as "the Criteria," which can be used to evaluate a proposed label Scheme.*
>
> *The Criteria, however, are intended for all industries and the language is subject to differing interpretations. They are not explicit about how to apply the requirements in a consistent manner to a Scheme or Schemes. Industry engagement in clarifying the criteria and their application will enable real world implementation of the requirements and provide valuable feedback to NIST.*
>
> *This document will formalize how to apply the Criteria to a given Scheme and how to evaluate a Scheme against the Criteria. For example, a scheme owner may use this document to evaluate that their cybersecurity testing scheme is conformant with the NIST criteria. When the scheme conformance is proven, they may obtain a license to issue the National Label to products compliant with their scheme.*

The document considers the scope of IoT Products,[44] which is broader in the NIST Criteria than just the hardware device. In the NIST Criteria, the IoT Product potentially includes, e.g., cloud services and hubs. On this point, here is the how this challenge is considered in section 6 of (draft) ANSI/CTA-2119:

> **6.2 Meeting IoT Product Requirements for Non-Device Components**
>
> As explained in Section 6.1, the full IoT Product is subject to conformity assessment under a Scheme that meets the Criteria. Further, an IoT Product includes the IoT Device (hardware) but often includes other Components, such as cloud services or a smartphone application.
>
> For these other Components, this Framework defines two paths by which a Scheme may meet the intent of the Criteria.
>
> **Type 1: Ensuring that the full IoT Product meets the Criteria by reference to the Criteria.**
>
> In this case, the Scheme shows that the specific requirements in the Criteria are met, through application of this Framework.
>
> **Type 2: Ensuring that the full IoT Product meets the Criteria by reference to the Criteria and to one or more trust marks.**
>
> In this case, rather than apply the Criteria to the Scheme and its ability to evaluate each Component, the intent of the Criteria is met by the trust mark requirements.
>
> Examples of trust marks might be:
>
> - For Cloud-based Components:
> - The Cloud Security Alliance STAR program (https://cloudsecurityalliance.org/star/)
> - Google's Cloud App Defense Alliance (https://appdefensealliance.dev/masa)
> - For smartphone applications:
> - Google's Mobile App Defense Alliance (https://appdefensealliance.dev/masa)
> - ioXt Alliance Mobile App Certification (https://www.ioxtalliance.org/certifying-your-device)

[44] The NPRM asks about scope and whether certifying "IoT Product" or "IoT Device" is appropriate. CTA's ANSI-accredited standards program operates as an open industry consensus body and includes CTA member companies and other private sector representatives. Currently, the working group is working through details of both IoT Product and IoT Device and is preparing a standard that speaks to both approaches. CTA, representing its members, believes the Program should start with IoT Devices and look to IoT Products as a potential future enhancement.

Definitions and References

A rigorous technical standard requires formal statements of contextual elements and accepted industry reference documents on citation. The (draft) ANSI/CTA-2119 document includes both normative and informative references. Examples of these normative references are as follows:

2.1.1 Normative Reference List

[1] National Institute of Standards and Technology (NIST), NIST IR 8425, *Profile of the IoT Core Baseline for Consumer IoT Products*, September 2022, https://doi.org/10.6028/NIST.IR.8425.

[2] 44 USC §3552(b)(3), available at https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title44-section3552&num=0&edition=prelim.

[3] ETSI EN 303 645 (V2.1.1) (2020-06): "CYBER; Cyber Security for Consumer Internet of Things"

…

Definitions in (draft) ANSI/CTA-2119 include cybersecurity terms of art, which must be used carefully to preserve the cybersecurity intent of the NIST team. In some cases, the definitions rely on NIST standards references; in others, industry standards; in others industry subject matter experts have provided the content. Numbers in square brackets (e.g., "[2]") are citations to normative references in the above normative reference section; [1] is therefore a citation to the NIST Criteria.

3.1 Definitions and Abbreviations

Authorized Entity	An entity permitted to access or manipulate the IoT Product. Examples may include the device owner, operator, manufacturer, ecosystem owner, IoT Product Components and services.
Authorized Individual	A person, such as the device owner, who is permitted to restore a device to a secure default (e.g., factory reset). This is more restrictive than Authorized Entity.
Best Practice Cryptography	Cryptography that is suitable for the corresponding use case and has no indications of a feasible attack with current readily available techniques.[3]
Consumer	Customer, end user, owner of the IoT product.
Consumer IoT Product	IoT products that are intended for personal, family, or household use.[1]

Customer	Organizations and individuals (page ii in Abstract of NISTIR 8259) ...who buy and use IoT devices [and] are intending to connect those devices to systems and networks, including the internet. (pg 7; 8259)
Criteria	The capabilities identified in NISTIR 8425, *Profile of the IoT Core Baseline for Consumer Internet of Things (IoT) Products* (see [1])
Globally Unique Identifier	A unique value associated with an endpoint. Uniqueness is universal, a Globally Unique Identifier is guaranteed to not collide with the Globally Unique Identifier of any other device. Note that Globally Unique Identifier is not the same as the RFC 4122 Universally Unique Identifier (UUID).

All of these (draft) ANSI/CTA-2119 sections are designed to support the purpose of the document: to provide a framework to evaluate a Scheme against the NIST Criteria.

The draft then takes each Criteria Capabilities component of NISTIR 8425 and defines assessment criteria for Schemes, as seen in the next section.

NIST Criteria Capabilities

Each "Capability" and its corresponding "Sub Criteria" in the NIST Criteria is represented in the document. Here is the Asset Identification capability section:

> **8.1 Asset Identification Capability Sub-criteria 1**
>
> *"The IoT product can be uniquely identified by the customer and other authorized entities (e.g., the IoT product developer)." [1]* [Editor: This is a quote from the NIST Criteria NISTIR 8425, cited as [1]. Each Capability is reviewed in a section that starts by quoting the relevant section of NISTIR8425.]
>
> **8.1.1 Assessment Outcomes**
>
> Scheme owner shall verify:
>
> a. That the IoT product has a Globally Unique Identifier that is available to authorized entities.

8.1.2 Scheme Requirement for Assessment

1. Functional test that the identifier meets the definition of a Globally Unique Identifier (may be limited to the number of units available and shall be combined with evidence from 8.1.1.3.)

2. Functional test that the Globally Unique Identifier can be obtained from the Product by authorized entities.

8.1.3 Scheme Requirement for Manufacturer Evidence

1. Evidence of how the manufacturer establishes a Product Identifier and ensures that it is a Globally Unique Identifier.

2. Evidence of how the manufacturer identifies the authorized entities that can access the Product Identifier.

8.1.4 Component Model Implications

1. At least one IoT Product Component of the IoT product shall meet this requirement.

2. When multiple components of the same model exist, each shall be uniquely identifiable.

3. The Globally Unique Identifier may or may not be considered protected data, depending on the method of generation and use case. For example, if the Identifier may be directly connected to a person or specific location, it would fall under the Data Protection criteria and need to be protected in an appropriate manner.

4. If access to the unique Product ID would potentially allow any increased risk for device compromise, it shall be protected by an appropriate security mechanism.

As noted, the above example from (draft) ANSI/CTA-2119 covers only one sub-criteria of one Capability, *Asset Identification Capability*. This level of detail is being developed for each of the sub-criteria of each of the other major Capabilities in NISTIR 8425 as well: *Product Configuration Capability, Data Protection Capability*, etc.

Annex B: Cybersecurity Label and QR Code Design

In this Annex we present draft material prepared by the Cybersecurity Label Design working group of CTA's ANSI-accredited standards program; this working group is designated "R14 WG7" in the CTA program. This group is a subgroup of the Cybersecurity and Privacy Management Committee (designated "R14").

The work of this group progresses. The material here is presented as an example of the form of the finished document. The final document will be ANSI/CTA-2120, *Design Requirements for a Label for IoT Device Cybersecurity*, and is anticipated for completion in the first half of 2024.

Label Design Overview

The document purpose is described in its section 5, Overview:

> Overview: This standard specifies a Technical Mark intended to be used as part of a Full Mark (which includes additional information). The Full Mark conveys to a consumer that the product meets certain cybersecurity requirements.
>
> Elements of the Full Mark include the following, listed hierarchically:
>
> { Full Mark:
> { Bounding Box:
> { Logo Zone:
> { FCC Trademark "Mark" *(* Note 1)* }
> }
> { QR Zone:
> { QR Code which encodes a URL}
> }
> { URL Zone:
> { URL in human-readable text }
> }
> }
> }
> *Note 1: The certification is out of scope for this document except as it defines allowable space.*

Layer 0: The Mark

The physical Mark, QR Code and URL are defined as "Layer 0" by this group. The Commission owns the certification Mark (shield and text "U.S. Cyber Trust Mark"). The Commission will specify requirements for use of this Mark *per se*. However, there are several additional details needed regarding QR coding and resolution, white space for accurate recognition of QR codes, and more. These details—outside the specifics of trademark usage—are covered in the (draft) ANSI/CTA-2120 document in this section. This part of the work is nearly complete.

The (draft) ANSI/CTA-2120 specifies detailed layout requirements for packaging designers, to ensure a common look and feel from manufacturer to manufacturer. Both horizontal and vertical layouts are covered, for different packaging requirements. The group has studied legibility, QR code error-correction level requirements, font size for human-readable text, and scaling for smallest usable sizes.

Diagrams show the relationship of these sections. Relative spacing requirements are supported by text sections.

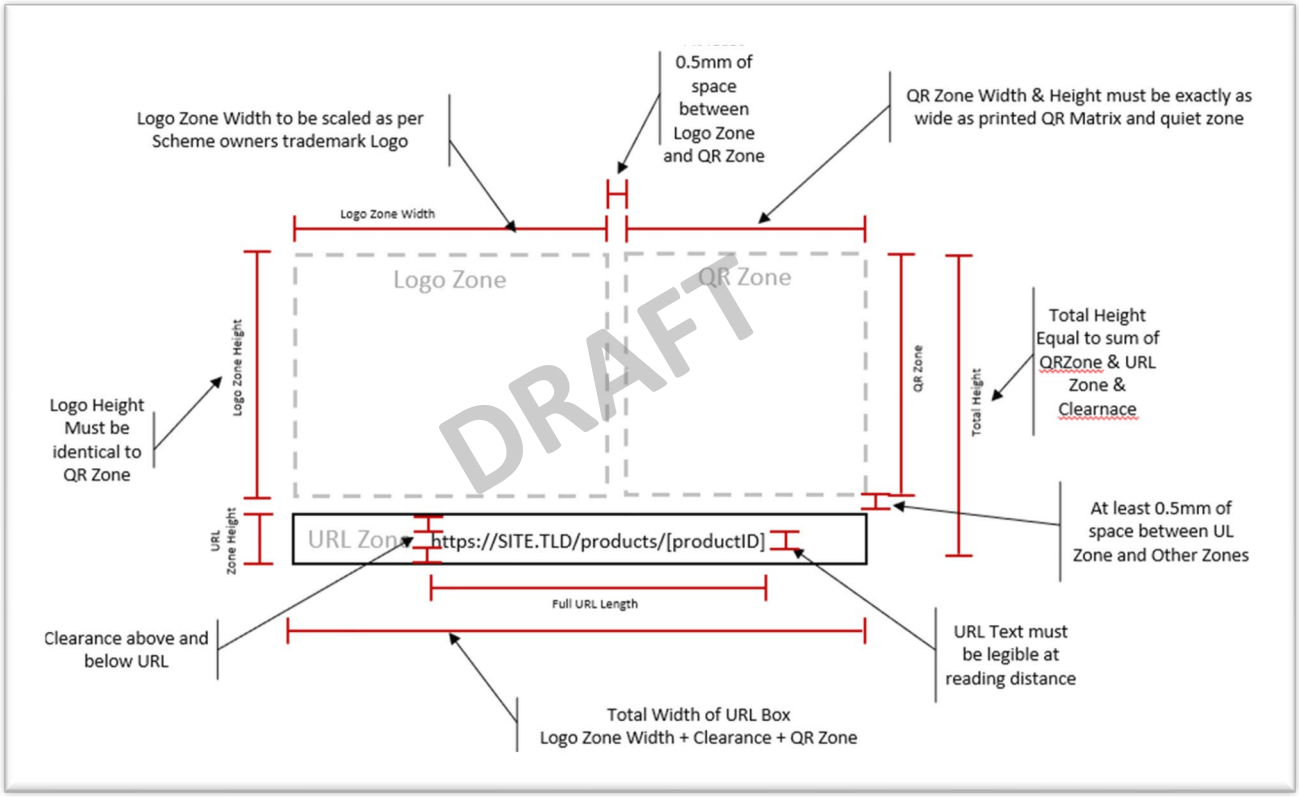

Figure 1:Layout of Mark, QR Code and URL

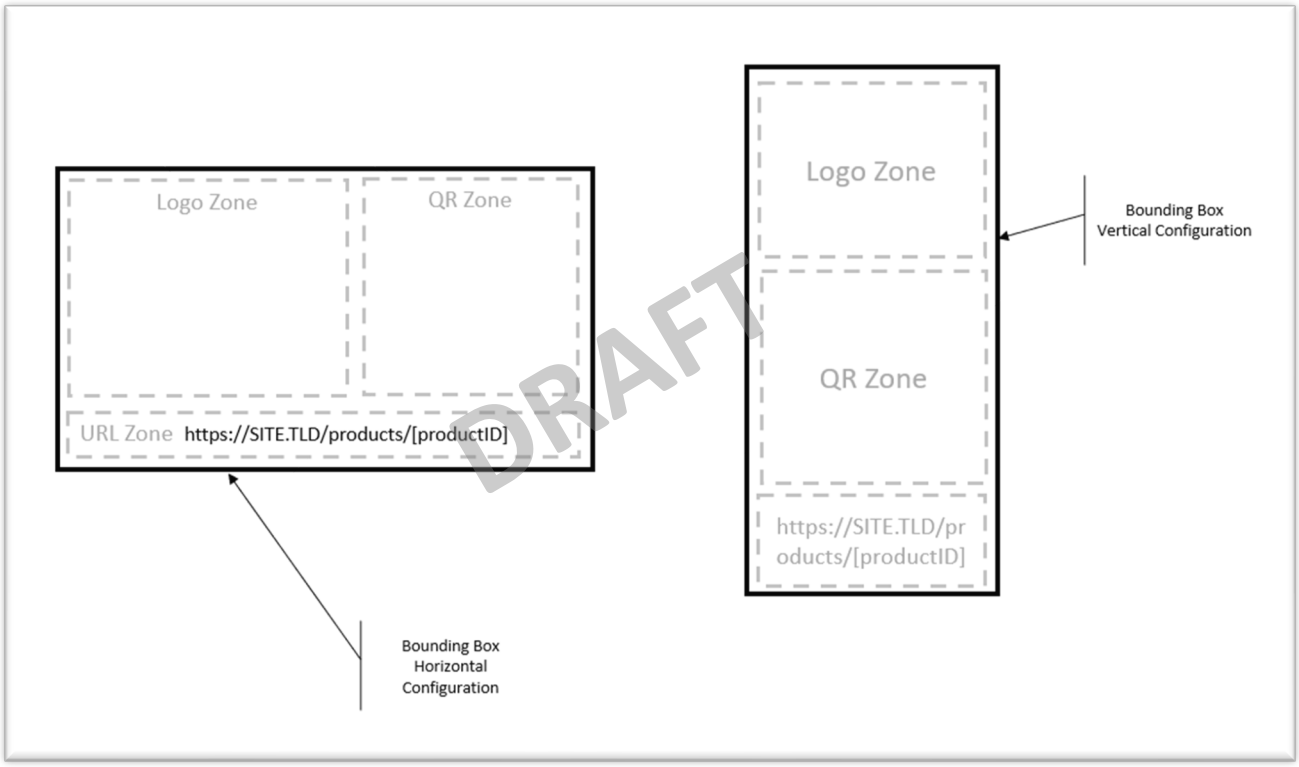

Figure 2: Bounding Box detail, horizontal and vertical layouts

Layer 1: Consumer Landing Page

The target of the QR Code is a consumer-friendly security details page, defined as "Layer 1". This work is in progress. The group has listed and prioritized the various candidate data fields to be presented on Layer 1. The NIST Criteria is the source of candidate fields, plus certain other data field types that arose in consumer testing by university groups and consumer advocates. Examples of fields expected to be on this page are:

- Security Updates: One of "Automatic", "Manual", "Consent-Based", "No Security Updates"; with attribute <expiration date> "Available until at least date"
- Access Control: One of "Password/factory default", "Password/user generated", "Biometric", "Multi-factor authentication", "No control over access", "Multiple user accounts", "Required user account", "Optional user account", "No user accounts"

These fields, and many more, were contributed by the Carnegie-Mellon CyLabs project team. (For simplicity here, some of the CMU CISPL version 1.0 encoding detail has been removed.)

Layer 2: Technical Landing Page

The Layer 1 landing page includes a link to the Layer 2 Technical Landing Page, for researchers and officials. This page's information is considered too technical or not interesting to consumers. This work is in progress and depends on the result of the Layer 1 determination.

Annex C: Regarding Trust Mechanisms

This material draws on CTA member company input (primarily manufacturers and retailers) and the work of CTA's R14 Working Group 8, Cyber Label Conformity and Trust Programs.

Overview: Trust Mechanisms

Several variations on Trust Mechanisms have been discussed. In the current NPRM record, there is a robust discussion of "certification" including "self-certification." Often, when the word "certification" is used, processes of accreditation and third-party review are involved. In such proposals, the "accreditation" can be read as accreditation by an internationally recognized accreditation body under ISO/IEC 17025/17065 and requirements for domain (cybersecurity and IoT) expertise. "Third-party review" would be of test results by the manufacturer in their accredited lab. There were also individual recommendations on requiring third-party testing for audit or market surveillance purposes, and that the manufacturer's test lab be "firewalled" in ways similar to CPSC rules. We believe these requirements would seriously hamper program adoption should they be the only means with which to participate in the Mark program.

We caution that all the above processes are different from what would be involved in "self-attestation." We ask the Commission to recognize this point in reviewing comments that recommend such processes in "self-certification."

Manufacturer's Self-Attestation

For the U.S. Cyber Trust Mark program, to establish trust and have the necessary legal foundation, a manufacturer's self-attestation process will require the following: It should have upfront qualification requirements, a license agreement with compliance terms, and per-product (or per-model line) requirements. We detail a proposal for this process below.

The NIST Criteria is foundational to the Mark program. Manufacturers who seek a license for self-attestation and use of the Commission's protected Mark should be required to provide documentation of how they meet all the elements of the NIST Criteria.

Some of these Criteria elements will be common to all the IoT devices within the corporation or within a corporation's product division. These elements will primarily be the NIST Criteria non-technical requirements, such as documentation of, "The vulnerability management policies and processes associated with the IoT product."[45]

Some elements will be NIST Criteria technical requirements, meaning specific design details of the IoT device, such as the requirement that, "The IoT product applies configuration settings to applicable IoT components."[46]

Therefore, since there are common (corporate or divisional practices) and distinct (IoT device) elements to consider as part of a contractual relationship, we recommend the following process. The version of this process outlined in steps 1-7 below is simplified to its most basic version. Certain options, such as License Scope, follow this list.

[45] *See* NISTIR 8425, section 2.2.2(1)(g).

[46] *See* NISTIR 8425, section 2.2.1(Product Configuration)(1).

Recommended Manufacturer Self-Attestation Process

These steps are recommended as the self-attestation process for a manufacturer in the U.S. Cyber Trust Mark program.

1. **FCC and Industry: Establish a Framework for assessing compliance to the NIST Criteria.**

The NIST Criteria is well-regarded and considered by many as the best foundation for this program. However, because the NIST Criteria is outcome-based, a corresponding list of compliance requirements is required. For the Framework, CTA recommends (draft) ANSI/CTA-2119 *Scheme Evaluation Framework* be incorporated by reference in the Mark program rules. Please see Annex A for more information on the draft Scheme Evaluation Framework.

2. **FCC: Develop a Mark Self-Attestation License agreement for manufacturers.**

To place the Mark on product packaging, and to protect the FCC's rights to the Mark, the FCC must create a license agreement giving compliant manufacturers the right to use the Mark. This agreement will include certain requirements on the participating manufacturer, including corporate-wide and per-product compliance to the NIST Criteria via the Framework described above, and usage requirements on the Mark. Use of the Mark on physical product packaging and on e-commerce web sites should be standardized. Significant work has gone into defining QR code details and landing page information details. (Draft) ANSI/CTA-2120 *Design Requirements for a Label for IoT Device Cybersecurity* is being developed specifically for that level of detail. Please see Annex B for more information on this document.

3. **Manufacturer: Apply for the Mark Self-Attestation License Agreement.**

Applications for the Agreement should include documentation, based on the Framework, of how the manufacturer will meet the corporate-wide elements of the NIST Criteria. After successful review of this material, the FCC and the manufacturer can execute the agreement.

4. **FCC: Review the NIST Criteria compliance documentation provided by the Manufacturer.**

The review should be based on a Framework as described above.

- On unsuccessful review, the FCC should notify the Manufacturer of the reason for unsuccessful review and means to correct.
- On successful review, the FCC notifies the Manufacturer of success and both parties proceed to execute the License Agreement.

5. **FCC and Manufacturer: Execute the Mark Self-Attestation License Agreement**

In this step, the FCC and manufacturer execute the Mark Self-Attestation License Agreement.

6. **Manufacturer: Document product compliance and prepare the Product Compliance Report**

The Manufacturer verifies a product design and documents the result in a Product Compliance Report. The manufacturer is responsible for holding the Product Compliance Report.

7. **FCC: As needed, request Product Compliance Report**

From time to time, the FCC may request a Product Compliance Report from the Manufacturer as part of market surveillance and audit processes.

Additional points:

- *License Scope*: License scope should be clearly identified as part of the agreement. Manufacturers should be permitted to execute and comply with the Mark Self-Attestation License Agreement on a corporate-wide basis, on a divisional basis, or for a specific product line.
- *License Authority*: The signatory party and administrator of the U.S. Cyber Trust Mark Self-Attestation program may be the Commission, or the Commission may delegate this

effort to a third-party License Authority. As many manufacturers are expected to seek self-attestation status, designating a third-party License Authority would be a prudent step.

- *NIST Criteria Partitioning*: The NIST Criteria non-technical and technical elements do not completely match the categories of "corporate" and "per-product". The Framework is a suitable place to identify which elements should be attested to in signing the license agreement, and which elements should be attested to in the per-product Test Report.

Verified Self-Declaration

Verified self-declaration (VSD) is similar to the self-attestation described above, but the manufacturer provides test results for review to an accredited third-party.

VSD is used by some tech industry alliances for their certification mark programs.

Third Party Conformity Assessment

This is sometimes referred to as "formal" conformity assessment ("formal CA"). These processes are supported by industry and by international bodies including the IEC Conformity Assessment activities.[47] When the Commission involves the process of formal CA, it may act as a national body to directly authorize schemes, or it may delegate this role to a separate entity.

CTA Recommendation: CTA recommends that both the Manufacturer Self-Attestation option described above, and formal third-party conformity assessment be options of the U.S. Cyber Trust Mark program. Formal third-party conformity assessment is likely to be chosen by manufacturers and their customers as market needs and risk assessment dictates. Where formal CA is used, industry-recognized processes should be used as intact as possible to preserve

[47] IEC, What is Conformity Assessment, (last visited Nov. 10, 2023), https://www.iec.ch/conformity-assessment/what-conformity-assessment.

characteristics of formal CA that are essential to international mutual recognition of this aspect of the Mark. Once these established processes are deviated from, it is no longer formal conformity assessment.

About Accreditation

Accreditation is a statement (attestation) from an independent third-party entity (Accrediting Organization) that specified requirements related to conformity assessment bodies have been met. ILAF and ILAC are international bodies of Accrediting Organizations. For third-party conformity assessment, the Program will require certain authorized third parties to have and maintain accreditation for ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*,[48] ISO/IEC 17065, *Conformity assessment: Requirements for bodies certifying products, processes and services*.[49] Both standards and the associated processes are well-known to Commission staff.

In addition, authorized third-party conformity assessment bodies (CyberLABs) will need to be verified for domain expertise. Domain requirements are sector-specific and here may include:

- Demonstration of technical expertise in Cybersecurity
- Demonstration of technical expertise with IoT
- (For sub-sectors) Demonstration of expertise with the sub-sector (e.g., "Drones")

This expertise, and the evaluation thereof, is not historically an area in which the Commission has participated. The Commission should authorize a third-party or parties to provide domain expertise review as needed.

[48] ISO, ISO/IEC 17025 – General requirements for the competence of testing and calibration laboratories, (2017), https://www.iso.org/publication/PUB100424.html.

[49] ISO, ISO/IEC 17065:2012 – Conformity assessment: Requirements for bodies certifying products, processes, and services, (2018), https://www.iso.org/standard/46568.html.