Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

COMMENTS OF CONSUMER TECHNOLOGY ASSOCIATION

J. David Grossman
Vice President, Regulatory Affairs

Mike Bergman
Vice President, Standards & Technology

Rachel S. Nemeth
Senior Director, Regulatory Affairs

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

October 6, 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
	)	

COMMENTS OF CONSUMER TECHNOLOGY ASSOCIATION

Consumer Technology Association (CTA)®[1] respectfully submits these 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] CTA agrees with the Commission's goal of enhancing cybersecurity for Internet of Things (IoT) products consumers use every day. The quickest way to meet this goal is a cooperative strategy that combines government criteria, industry consensus standards and existing industry certification processes. The resulting transparency will allow consumers to make wise buying choices and encourage device makers to meet established cybersecurity standards.

I. INTRODUCTION AND SUMMARY

Over the last decade, IoT has become integral to how we live, work and play. More than 100,000 attendees saw at CES this year how IoT applications are enhancing efficiency and improving functionality across nearly every sector of our economy, including healthcare, transportation, energy, communications, agriculture and more. As explained by CTA president and CEO Gary Shapiro, "[r]esearch shows consumers want more information on the safety and

[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 influential tech event on the planet.

[2] *Cybersecurity Labeling for Internet of Things*, Notice of Proposed Rulemaking, FCC 23-65 (rel. Aug. 10, 2023) ("*NPRM*").

security of their connected devices, and we agree."[3] The U.S. Cyber Trust Mark ("U.S. Cyber Trust Mark" or "Mark") has the potential to be a successful public-private collaboration, helping to increase security while allowing for innovation. The Mark will enable manufacturers to distinguish more secure products in the marketplace and empower consumers to demand securable IoT.

As IoT proliferates, industry and policymakers have recognized the ways in which increased connectivity expands the ever-shifting threat landscape and responded to address these threats. Once-harmless devices like printers and baby monitors can be conscripted into botnets that conduct massive "distributed denial of service" (DDOS) attacks. The scale of global IoT devices (estimated to reach 80 billion devices by 2025) provides an unprecedented and attractive threat vector for bad actors who can use relatively cheap exploits to obtain rewards.[4] Put another way, "[w]hile IoT makes our world better, it also tempts bad actors to exploit consumers' connected devices. Tech makers take this threat seriously and are building and enhancing tools to improve product security and protect consumers."[5]

CTA and its members have made enhancing security across the IoT ecosystem a top priority. In 2018, CTA joined forces with partners across the connected ecosystem to form the Council to Secure the Digital Economy (CSDE) and develop guidance for the international information and communications technology community on how to secure IoT and reduce risk

[3] Press Release, CTA, Consumer Technology Association Joins White House to Support Cybersecurity Labeling Program to Protect Consumers from IoT Attacks (July 18, 2023), https://www.cta.tech/-Resources/Newsroom/Media-Releases/2023/July/CTA-Joins-White-House-IoT-Labeling-Program.

[4] Council to Secure the Digital Economy ("CSDE"), *International Botnet and IoT Security Guide*, at 3 (2021), https://kvh31b.p3cdn1.secureserver.net/wp-content/uploads/2021/03/CSDE-2021-Botnet-Report-March-24-2021.pdf.

[5] Gary Shapiro, *Consumers Want to Know More about IoT Security. A New Public/Private Labeling Program Will Help*, CTA (July 18, 2023), https://www.cta.tech/Resources/Articles/2023/Consumers-Want-to-Know-More-about-IoT-Security-A-N.

across the connected ecosystem.[6] As part of this effort, the CSDE "convened the convenors," bringing together trade associations, standards organizations, industry alliances and coalitions to develop the broadest and most technically deep industry consensus on IoT security worldwide.[7] Collectively, the "C2" participants represented thousands of companies and many different segments of the global digital economy, leveraging input from hundreds of security professionals. Based on the principle that the best way to achieve IoT security is for technical experts to develop and advance security specifications that will disseminate throughout the global market, the C2 Consensus provides clear expert guidance to industry and government for securing new IoT devices to raise market expectations for security and advance global policy harmonization.

The U.S. Cyber Trust Mark program can be an important next step towards advancing IoT security, building on longer term efforts of technical experts in industry and government. Over the last six years, the U.S. government has partnered with industry to cultivate the goals that lie at the heart of the U.S. Cyber Trust Mark. Built from consecutive policy steps—from the 2018 Botnet Report to the IoT Cybersecurity Improvement Act of 2020 to Executive Order 14028 and ultimately NISTIR 8425—the U.S. Cyber Trust Mark program is poised to provide clear and evolving expectations for minimum cybersecurity capabilities in IoT devices. The program will empower consumers—and retailers, and enterprises, and systems integrators—to have available tools to make purchasing decisions based on security and position the United States to lead the way in IoT cybersecurity policy going forward.

[6] *See generally* CSDE, Cyber Resources, https://csde.org/news-resources/ (last visited Sept. 30, 2023).

[7] CSDE, *The C2 Consensus on IoT Device Security Baseline Capabilities*, at 1 (2019), https://kvh31b.-p3cdn1.secureserver.net/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf.

CTA offers a few foundational recommendations for successful implementation of the U.S. Cyber Trust Mark program:

- The top-line goal of the program should be to reduce systemic cybersecurity risk to internet infrastructure and to users of connected devices.
- The structure of the program should enable the U.S. Cyber Trust Mark to effectively meet key goals of empowering consumers to demand securable products, incenting manufacturers to meet baseline cybersecurity requirements and fostering harmonized cybersecurity expectations across the global connected ecosystem.
- As the government has recognized,[8] this program must be voluntary to ensure the broadest reach, most efficiency and widest access to the valuable diversity of IoT technologies finding new ways to meet consumer needs each day.
- Important both for speed and for ultimate success is building the program on a robust foundation of existing National Institute of Standards and Technology (NIST) guidance, global standards and certification processes aligned to the NIST Criteria.
- To ensure the success of such a voluntary program, the Commission must incorporate strong incentives for manufacturer participation, educate consumers on the Mark and how to use the label, prioritize verified self-attestation and safeguard trust in the integrity of the program through objective, transparent and rigorous processes.
- 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.

We elaborate on these initial recommendations below.

II. THE U.S. CYBER TRUST MARK PROGRAM SHOULD ADDRESS THE KEY GOALS OF IOT CYBERSECURITY LABELING

The U.S. Cyber Trust Mark program should be structured to address primary risks and harms to consumers, infrastructure and national security. Specifically, IoT cybersecurity labeling aims to empower consumers to make informed purchasing decisions, incentivize manufacturers to include baseline security capabilities in IoT products and—in doing so—reduce the

[8] *See NPRM* ¶ 9.

ecosystem-wide (horizontal and vertical) risks posed by insecure IoT.[9]

A. The Primary Goal of the Program Should Be to Reduce Systemic Cybersecurity Risk to Internet Infrastructure and to Users of Connected Devices

A foundational document for the IoT cybersecurity labeling program is NISTIR 8425, the "Consumer Profile" that sets baseline capabilities by defining expected outcomes.[10] The consensus baseline capabilities in NISTIR 8425 aim to reduce horizontal risk (like botnets and DDOS attacks), reduce vertical risk (like attacks on specific enterprises conducted via insecure devices on the intranet) and make IoT devices more securable within their connected environment. NISTIR 8425 articulates minimum capabilities, while the label and individual marketing efforts can inform consumers of the unique or more sophisticated security capabilities a consumer may choose to purchase based on their particular needs. NISTIR 8425 strikes a careful balance between (i) establishing a baseline set of capabilities to inoculate devices against most risk and (ii) not raising the floor so high that valuable devices are priced out of the market or cannot be designed at the necessary size and scale for their function because they are required to incorporate security features they do not need or that can be incorporated in other parts of their environment.

The U.S. Cyber Trust Mark program cannot and should not be construed as preventing *all* risk or assuring that a device is impervious to every possible attack. The IoT cybersecurity consumer label envisioned in NISTIR 8425 is not designed to prevent harmful interference or

[9] *See, e.g., id.* ¶ 2 (proposing a voluntary cybersecurity labeling program "[t]o provide consumers with the peace of mind that the technology being brought into their homes is reasonably secure, and to help guard against risks to communications").

[10] Michael Fagan, Katerina Megas et al., *Profile of the IoT Core Baseline for Consumer IoT Products, NIST IR 8425*, NIST (Sept. 2022) ("NISTIR 8425"), https://nvlpubs.nist.gov/nistpubs/ir/2022/-NIST.IR.8425.pdf.

eliminate all possibility of horizontal or vertical risk (e.g., risk to the specific environment or network in which the device is deployed). As the *NPRM* and NIST guidance recognize, cybersecurity is a shared responsibility, and IoT devices alone cannot manage all cybersecurity risk to an enterprise or the network.[11]

Horizontal risk—of devices being compromised and turned into "bots", regardless of the original design, application or installation—is a significant threat to be addressed here. Botnets are responsible for huge numbers of DDoS attacks on U.S. infrastructure, including critical infrastructure. Botnets scan for vulnerable networks and install malware, including ransomware. DDoS attacks and ransomware are two of the most significant ongoing and pervasive problems in cybersecurity today. The United States is the largest target of DDoS attacks.[12] Ransomware attacks are at an all-time high, and the U.S. shoulders the brunt of these attacks.[13]

The reason for this growth is that botnets are profitable. Malicious actors have financial incentives to attack connected devices. DDoS attacks are bought and sold on the dark web. Ransomware-as-a-Service (RaaS) is a growing business, and extortion and payment demands can be in the millions of dollars.[14] The original baseline effort by NIST was driven by concern over horizontal risk—and botnets in particular—for these reasons and the challenge has only grown exponentially. And when addressing horizontal risk, vertical risk is also addressed. The U.S.

[11] *See NPRM* ¶ 53; NIST, *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products [White Paper]*, at 19 (Feb. 4, 2022) ("NIST Recommended Criteria"), https://-nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf.

[12] Omer Yoachimik & Jorge Pacheco, *DDoS threat report for 2023 Q2*, Cloudflare (July 18, 2023), https://blog.cloudflare.com/ddos-threat-report-2023-q2/.

[13] Malwarebytes, Threat Intelligence Team, *2023 State of Ransomware* (Aug. 3, 2023), https://www.-malwarebytes.com/blog/threat-intelligence/2023/08/global-ransomware-attacks-at-an-all-time-high-shows-latest-2023-state-of-ransomware-report.

[14] Clare Stouffer, *Ransomware statistics: 102 facts and trends you need to know in 2023*, Norton Blog (Aug. 8, 2022), https://us.norton.com/blog/emerging-threats/ransomware-statistics.

Cyber Trust Mark program should focus on addressing these systemic risks to U.S. critical infrastructure, enterprises and individuals.

The IoT labeling program should *not* focus on reducing harmful interference caused by compromised devices. While there are examples of such problems, the consequences are completely dwarfed by the potential of botnets. Examples of a cybersecurity attack causing harmful interference do exist, but history does not show that such attacks are anywhere near as prevalent as botnets.[15] And a harmful interference attack executed at scale—such as many connected devices being reprogrammed to cause interference—is by definition a botnet attack. A focus on reducing systemic cybersecurity risk will lead to reduced DDoS attacks, decreased distribution of malware, and reduced risk of at-scale harmful interference attacks.

B. The Commission's Program Will Be a Clear Indicator that a Device Incorporates Reasonable Cybersecurity Practices

A second key goal of the U.S. Cyber Trust Mark program, as explained in Section IV, is providing meaningful assurance to consumers and regulators that IoT devices that have earned the Mark incorporate "reasonable" cybersecurity practices. The Commission can accomplish this goal by explicitly and adequately enforcing the program's integrity as a genuine measure of the security of the device. That goal is best accomplished by aligning with and building upon the NIST and private sector work that has been ongoing for half-a-decade and has broad support.

CTA is hopeful for a speedy and effective deployment of the voluntary U.S. Cyber Trust Mark program by the Commission and within its legal jurisdiction.

[15] *See NPRM* ¶ 63.

C. The Commission Has the Legal Authority Necessary to Establish This Voluntary Consumer Labeling Program

The Commission can adopt this voluntary IoT labeling program based on its authority under Section 302 of the Communications Act to "consistent with the public interest, convenience, and necessity, make *reasonable* regulations… governing the interference potential of devices."[16] As discussed above, though NIST's baseline capabilities and IoT cybersecurity labeling program criteria are not designed to specifically address the risk of harmful interference, IoT devices that meet these requirements will be better prepared to defend against cybersecurity attacks aimed at causing harmful interference should they occur at some point. Therefore, the Commission's proposal to establish rules that would set forth the IoT security standards, compliance requirements and operating framework for this *voluntary* labeling program fall within the scope of the FCC's Section 302 authorities.

Rules establishing a voluntary labeling program would be a "reasonable" approach to guard against the possibility of a cyber-attack causing harmful interference, while also promoting widespread public-private interest in incentivizing more ubiquitous cybersecurity capabilities across IoT devices. Adopting rules to effectuate the transparent, uniform administration of this voluntary labeling program as a natural extension of years of government-industry collaboration—based on the consensus guidance developed by NIST in accordance with the IoT Cybersecurity Improvement Act and Executive Order 14028—is reasonable to implement the program. To achieve a meaningful label for consumers, IoT devices bearing the Mark must be subject to common, objective expectations which can only be uniformly established by the owner

[16] *See* 47 U.S.C. § 302a(a) (emphasis added); *NPRM* ¶ 57 (tentatively concluding that the FCC may adopt the program pursuant to Section 302 of the Communications Act).

of the Mark (i.e., the FCC, pending the U.S. Trademark Office's approval of the FCC's application).

Section 302, however, is not a broad grant of authority to address IoT security writ large through prescriptive regulatory requirements. Section 302 does not speak to the core focus of the program—incentivizing consumer IoT devices to meet common baseline cyber requirements—and if the FCC were to adopt rules requiring IoT devices to achieve the Mark (e.g., as a prerequisite of equipment authorization), it would be acting beyond its authority. Indeed, a mandatory program would not be consistent with the public interest, convenient or necessary for adopting reasonable regulations for the purposes of Section 302.[17]

Of note, the Commission's lack of authority to prescribe cybersecurity requirements has not inhibited its ability to meaningfully support the nation's national security and cybersecurity interests, especially through reliance on collaboration with industry. The Communications Security, Reliability, and Interoperability Council (CSRIC) has made invaluable strides over the last decade to address complex communications security issues and to identify and promote common practices for addressing those challenges. In cases where Congress has seen the need for mandatory requirements, it has swiftly (and in a bipartisan manner) passed legislation directing the FCC to act.[18] At this stage, Congress has not directed the Commission to impose mandatory regulatory requirements to address IoT security – however, the Commission has the

[17] As stakeholders have relayed to the Commission before, incorporating IoT security into the equipment authorization process would "highly disruptive and damaging to th[is] process." Letter of Jennifer Tatel and Clete Johnson to Chairwoman Rosenworcel and Commissioners, ET Docket No. 21-232, EA Docket No. 21-233 at 4 (filed Sept. 14, 2021).

[18] *See e.g.*, Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601-1609; Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 134 Stat. 158 (2020)) (Secure Equipment Act).

authority necessary to stand up and administer this voluntary labeling program and will build on a strong foundation of bipartisan, public and private support in doing so.

A well-structured voluntary labeling program that aligns incentives for participation will receive widespread support across the IoT community.

III. BASING THE THRESHOLD FOR EARNING THE MARK ON NIST GUIDANCE THAT LEVERAGES INDUSTRY EXPERTISE WILL MOST EFFECTIVELY AND EFFICIENTLY MEET THE GOALS OF THE PROGRAM

To establish the U.S. Cyber Trust Mark program with speed and efficiency, the Commission should build the program on the robust guidance developed by NIST pursuant to the IoT Cybersecurity Improvement Act and Executive Order 14028, and the agency should leverage the unique expertise and existing certification infrastructure offered by well-regarded industry organizations. If the Commission successfully builds the U.S. Cyber Trust Mark on this multi-year foundation of policy development and technical implementation, CTA expects that the program will receive strong support and widespread participation.

A successful U.S. Cyber Trust Mark program will leverage existing infrastructure that stakeholders have developed to support the program, including robust processes for certifying IoT security and NIST guidance regarding the label and baseline requirements. With this in mind, the scope of the program should reflect the scope envisioned by NIST, meaning that the Commission does not need to modify the NIST definition of IoT device. The *NPRM*'s question of whether and how to focus the program on IoT "products" versus "devices" requires further consideration, and CTA's recommendation is to focus on IoT devices at this time. CTA's R14 Working Group 6 intends to provide a recommendation on how IoT products may be handled as the Mark program evolves. This should not delay the FCC's implementation of the program for IoT devices. Throughout its administration of the U.S. Cyber Trust Mark program, the

Commission must balance the need for scalability and efficiency with the need to ensure consumer and governmental confidence in the integrity of the label.

The program rules should clarify that an IoT device outside the scope of the program is not eligible to achieve the Mark. As the Commission suggests, scope is an important qualifier as to whether a submission may be considered in the program and recorded in the program's public registry.[19] A submission that does not fit the scope is unlikely to fit well in the Mark's product registry, as search keys and other design elements may not fit such cases.

A. The Scope of the U.S. Cyber Trust Mark Program Should Reflect the Scope Envisioned in NIST's Recommended Criteria

1. NIST Criteria Should Form the Base of Technical Criteria for the U.S. Cyber Trust Mark Program and NIST Should Update/Maintain that Criteria Over Time

The Commission should base the technical criteria requirements for an IoT device to achieve the U.S. Cyber Trust Mark on the NIST Criteria (currently articulated in NISTIR 8425 and Appendix A of the *NPRM*) and the supporting body of work that preceded NISTIR 8425, including the NISTIR 8259 series[20] and the NIST white paper.[21] In addition, NIST should be responsible for updating and maintaining the Criteria throughout the life of the program as threats, technologies and best practices evolve. This approach is consistent with previous direction from both Congress and the Administration, which have recognized NIST's subject matter expertise by separately and consistently directing NIST to develop baseline cybersecurity capabilities, labeling criteria and related IoT security guidance. For example, the IoT Cybersecurity Improvement Act directed NIST to develop baseline capabilities (NISTIR 8259)

[19] *See NPRM* ¶¶ 12-14.

[20] NIST, Cybersecurity for IoT Program, *NISTIR 8259 Series* (last updated Nov. 16, 2021), https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series.

[21] NIST Recommended Criteria.

and a federal profile for NISTIR 8259.[22] The Administration directed NIST to develop IoT security labeling criteria (NISTIR 8425) via Executive Order 14028[23] and subsequently directed NIST to develop requirements for consumer-grade routers to be incorporated into the FCC's U.S. Cyber Trust Mark program.[24]

Maintaining NIST as the central repository for developing and maintaining this guidance will support consistency across sectors utilizing IoT and ensure a whole-of-government approach. The IoT Cybersecurity Improvement Act also directed the Office of Management and Budget to incorporate NIST's guidance regarding minimum cybersecurity capabilities for IoT into federal procurement rules, which define the government's minimum cybersecurity expectations across civilian federal agencies.[25] Ensuring that the U.S. Cyber Trust Mark baseline requirements remain aligned to these federal procurement requirements will foster synergy between the programs and harmonize security risk management between the federal government and commercial sector. Likewise, as agencies like the Department of Energy develop sector- and use-case-specific criteria (e.g., for smart meters and power inverters),[26] NIST will be well positioned to integrate those criteria into the overarching requirements for the program.

[22] IoT Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207, § 2, 134 Stat. 1001, 1001 (2020).

[23] Executive Order No. 14028 of May 12, 2021, Improving the Nation's Cybersecurity, 86 Fed. Reg. 26633 (May 17, 2021).

[24] Statements and Releases, The White House, *Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers* (July 18, 2023), 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/.

[25] IoT Cybersecurity Improvement Act of 2020 § 2.

[26] Department of Energy, *Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid* (Oct. 2022), https://www.energy.gov/sites/default/files/2022-10/Cybersecurity%20Considerations%20for%20Distributed%20Energy%20Resources%20on%20the%20U.S.%20Electric%20Grid.pdf.

2. The Commission Does Not Need to Modify the Program's Scope with Proposed Changes to NIST's Definition of IoT Device

The Commission does not need to modify NIST's definition of IoT device, and doing so could negatively impact the efficacy of the U.S. Cyber Trust Mark program. The *NPRM* proposes to modify NIST's definition of IoT device to include the following underlined language:

> (1) an Internet-connected device capable of intentionally emitting RF energy that has at least one transducer (sensor or actuator) for interacting directly with the physical world, coupled with (2) at least one network interface (e.g., Wi-Fi, Bluetooth) for interfacing with the digital world.[27]

Focusing the scope of the U.S. Cyber Trust Mark program on intentional radiators of RF would unnecessarily omit wired devices, which should also be part of the program. Such focus would also deviate from NIST's definition, which was developed through extensive industry collaboration. This new scope would cause the FCC's program to diverge from the rest of the government's approach.

Consistent with NIST's definition, certain classes of devices should be out of scope for the Commission's consumer IoT labeling program. For example, NIST excludes common general purpose computing equipment (e.g., personal computers and smartphones) as well as general internet and networking infrastructure (e.g., internet routers and switches) from the scope of its recommended criteria.[28] At this stage, routers should also be out of scope for the program because NIST is working to develop separate criteria targeted to address their unique security considerations. In the current program, as per EO 14028, NIST has defined a "consumer profile" in NISTIR 8425, and therefore industrial IoT applications must be treated as out of scope for the

[27] *NPRM* ¶ 11 (emphasis added).

[28] *See* NIST Recommended Criteria at 3 n.3.

consumer labeling program as the work effort did not take their specific characteristics into account.

3. THE PROGRAM SHOULD INITIALLY FOCUS ON CERTIFYING IOT "DEVICES" AS STAKEHOLDERS CONSIDER WHETHER AND HOW TO CERTIFY MORE COMPLEX IOT "PRODUCTS"

The program should focus on certifying only "IoT devices" at this stage. This approach will enable the FCC to establish the U.S. Cyber Trust Mark program quickly and efficiently with processes that already meet the requirements of the NIST guidance and criteria, pressure test the program and expand the program to include more complex products with the benefit of more time, experience and stakeholder input.

CTA agrees that components of an IoT product beyond the hardware device itself impact the security of the IoT product and its ability to achieve the outcomes defined in NISTIR 8425. Examples of such non-hardware aspects of an IoT product include related smartphone apps, cloud services and hubs. For this reason, in its Labeling Criteria, NIST defines "IoT product" as "an IoT device and any additional product components that are necessary to use the IoT device beyond basic operational features." NIST focuses the criteria on "IoT product" because additional components (e.g., specialty networking/gateway hardware, companion application software and backends) can introduce new or unique risks to the IoT device, so the entire IoT product—including auxiliary components—must be securable.[29]

As a practical matter certifying an IoT product is more complicated than certifying solely the IoT device. CTA recognizes this challenge and is developing recommendations in R14 Working Group 6 for defining boundaries and procedures that would enable the Cyber Trust Mark program to include an IoT product at a future date, consistent with NIST guidance. An

[29] *See id.* at 3-4.

example of the complexity is that app, cloud and platform providers are often different entities than the IoT product producer, which can complicate and delay the conformity assessment process. As cloud services and platforms may not be bespoke for IoT products, such providers may face different incentives for engaging with the U.S. Cyber Trust Mark program. The work in progress under Working Group 6, consistent with NIST guidance in those meetings, would be that the components of an IoT product *in combination* must meet NISTIR 8425—so the IoT product provider could work through the program's assessment procedures and attest that its product's components meet program requirements.

Still, other aspects of an IoT product may require additional guidance to be adequately addressed in the U.S. Cyber Trust Mark program. As NISTIR 8425 states, "[p]roduct criteria are recommended to apply to the IoT product overall, as well as to each individual IoT product component, as appropriate. Most criteria concern the IoT product directly and are expected to be satisfied by software and/or hardware means implemented in the IoT product."[30] However, a hardware device has distinct security considerations from cloud services and mobile applications; thus, to ensure the security of these components each of these categories likely will require distinct technical standards and certification schemes themselves. Given the complexities, further attention is required, and CTA has convened experts for this purpose. The FCC should await the anticipated guidance of R14 Working Group 6 before deciding whether and how to extend the scope of the program in this regard.

At a later date, it may also be appropriate to review the role of modules and chips, which make up an "IoT device," because some such components will have features that allow the device to meet some of the requirements in the NIST Criteria. A later feature of the Mark

[30] *See* NISTIR 8425 at 3-4; *see also* NIST Recommended Criteria at 4.

program may be some form of pre-qualification or pass-through. CTA recommends deferring consideration of this capability to when the basic Mark program is established.

B. A Successful U.S. Cyber Trust Mark Program Will Leverage Existing NIST and Industry Processes

CTA appreciates the FCC's recognition that close partnership and collaboration between the federal government, industry and other stakeholders is vital to ensuring the success of the proposed program, and that a collaborative environment leveraging the expertise, incentives and authority of various constituencies will allow for the swift establishment and maturity of the program with broad industry and consumer acceptance.[31] Fortunately, industry organizations already have robust processes in place to approve IoT devices in line with NIST guidance and international standards. The Commission should leverage these processes and build the labeling program requirements on NIST's guidance to establish the program quickly and efficiently.

1. Industry Organizations Already Have Robust Processes in Place to Assess IoT Device Security In Line with NIST Guidance and International Standards

As envisioned in the *NPRM*, the Commission will serve as the overall program administrator for the U.S. Cyber Trust Mark.[32] In this role, the FCC will own and license use of the trademarked U.S. Cyber Trust Mark logo. The Commission will also be responsible for decisions regarding (i) the programmatic process, (ii) the levels of assurance and trust mechanisms the program requires (including processes to vet third-party administrators, CyberLABs and IoT themselves), (iii) label development and associated information and (iv) consumer outreach and education (ideally in partnership with CISA and other pertinent

[31] *NPRM* ¶ 19.

[32] *Id.* ¶ 22.

stakeholders). For many of these activities, the Commission will benefit from the expertise of organizations that already perform these types of functions.

In addition to the FCC as program administrator, CTA sees several distinct categories of stakeholders with key roles in the U.S. Cyber Trust Mark program, including: (i) standards development organizations, (ii) accreditation bodies, (iii) conformity assessment entities, and (iv) NIST. The program may also include (v) a licensing authority (a third party contracted by the FCC to authorize conformity assessment entities and manufacturers utilizing self-assessment and self-approval processes) and (vi) a registry operator. Indeed, a successful U.S. Cyber Trust Mark program will utilize existing processes from NIST and Commission-designated third-party administrators, including:

- NIST, through well-defined and well-respected multistakeholder processes, to develop and maintain program criteria for the various sectors, such as NISTIR 8425 for consumer IoT;

- Accredited standards development organizations to adapt cybersecurity standards to align with the NIST Criteria;

- Scheme owners to incorporate aligned standards as requirements for their Schemes,

- Schemes to be evaluated against the Criteria by interpretive guidance developed in a consensus manner, such as CTA-2119 Scheme Evaluation Framework;

- The International Accreditation Forum (IAF) and International Laboratory Accreditation Cooperation (ILAC) to accredit labs and conformity assessment organizations as needed, with requirements established by consensus between the Commission and industry;

- CyberLABs, independent third-party conformity assessment bodies accredited against consensus requirements, including potentially ISO/IEC 17065 and/or ISO/IEC 17025 and consensus guidance from industry;

- Industry alliances authorized to act as CyberLABs to certify products; and

- Manufacturers who will provide documentation concerning self-assessment to achieve the Mark.

Housing and owning every aspect of this program within the Commission’s walls will be unwieldy, create potentially duplicative and contradictory requirements, and delay the start of the program. Importantly, the process of developing security requirements and standards, which is most effectively conducted by industry, takes significant time and is already underway for purposes of the U.S. Cyber Trust Mark. Leveraging this ongoing work will speed the establishment of the program and increase the program's ultimate quality. Specifically:

- The Commission should determine the programmatic rules, i.e., how the U.S. Cyber Trust Mark program will operate, the management and division of responsibility for certifying to and using the Mark, the level of assurance required, etc. This process involves policy decisions and value judgements about the trust mechanisms needed to ensure public confidence in the program. Such rules are not likely to require frequent updates and, as a result, are well suited to Commission-level rulemaking process.

- NIST should update and maintain the baseline cybersecurity capabilities/desired outcomes, i.e., the minimum cybersecurity capabilities that a device/product must meet to achieve the U.S. Cyber Trust Mark, articulated in NISTIR 8425. These requirements have been developed through the substantial subject matter expertise at NIST and across its broad, diverse set of stakeholders. They will likely evolve with some regularity over the life of the program and require mapping/integration with sector- and use-case specific criteria developed by other expert agencies. Industry broadly supports NIST in this role, and Congress and the Administration have recognized that NIST's nimble process and established expertise are well-suited to this task.

- Approved/accredited industry bodies should develop and maintain technical (conformity assessment) standards, i.e., what technical requirements must a device meet to certify that they meet the baseline cybersecurity capabilities. As the Commission has recognized in other contexts (such as equipment authorization), industry organizations and the companies producing these technologies are best positioned to update technical standards as the landscape evolves. Cybersecurity is a rapidly shifting field and the technical standards on which the U.S. Cyber Trust Mark is based must be able to quickly evolve and encourage IoT providers to innovate forward rather than comply backward.

- Approved/accredited industry bodies – independent third-party entities and industry alliances – should provide an option for testing and certifying products against technical requirements (conformity assessment).

- Manufacturers meeting specific documentation requirements should be permitted to self-assess their own products to qualify for the Mark. A number of manufacturers have implemented secure-by-design and secure-by-default processes for their products. To scale the program quickly and to gain the support of these best-in-category entities, self-attestation to use the Mark must be an option in the program.

Tailoring various types of decision-making to the forums best suited to make them over the life of the program will support an efficient and effective process for developing and maintaining the U.S. Cyber Trust Mark.

2. THE COMMISSION SHOULD RELY ON NIST BASELINE CAPABILITIES AND RECOMMENDED LABELING CRITERIA TO FORM THE LABELING PROGRAM REQUIREMENTS

To the maximum extent possible, the U.S. Cyber Trust Mark should maintain a common baseline across IoT products, and NIST should remain the central hub for developing and maintaining the IoT labeling criteria.[33] As discussed above, Congress and the Administration have directed that NIST act as the government's subject matter expert and, as a practical matter, NIST has substantially more staff with expertise who are already dedicated to this work. The Commission does not have the luxury of convening stakeholders to develop technical criteria with the same reach and rigor as NIST. Should the FCC seek to convene stakeholders for this work, the Federal Advisory Committee Act (FACA) may limit robust engagement from all relevant stakeholders as membership and participation in such committees are bound by nominations and FCC approval.[34] Further, NIST has spent five years developing the body of work that culminates in NISTIR 8425. ISO/IEC's Joint Technical Committee 1 has spent a similar time developing the ISO/IEC 27402 baseline standard. These topics are complicated and take significant time to develop correctly. CTA does not recommend convening stakeholders for a new effort, especially as there is a significant body of work from NIST and industry already available for use.

[33] A whole-of-government effort does not mean that all agencies are prohibited from establishing specific criteria within their expertise, but it should be thoughtfully done and with coordination. For example, the Administration envisions tailoring specific criteria to consumer routers, smart meters and power inverters. The White House Statements and Releases, *supra* note **Error! Bookmark not defined.**.

[34] *See* FACA, as amended, 5 U.S.C. 10.

The Commission should avoid adding technical criteria on its own to the U.S. Cyber Trust Mark program. For example, the *NPRM* proposes to require that manufacturers disclose the guaranteed minimum support period for an IoT device or product, during which the manufacturer commits to identify and patch security vulnerabilities in the product.[35] Although CTA agrees this type of communication may be valuable to consumers, such a requirement overlaps with existing elements of the proposed program as well as established coordinated vulnerability disclosure (CVD) practices.[36] NISTIR 8425 already includes criteria regarding software updates and related information dissemination, based on language developed by cybersecurity subject matter experts. This includes language specific to cybersecurity, such as noting that the software of all IoT product components can be updated by "authorized" individuals and each IoT product component can receive, verify, and apply "verified" software updates.[37] The words "authorized" and "verified" are terms of art in this context, and conformity requirements require careful and expert consideration. There are similar challenges in attempting to define "critical" in the context of "must address critical patches." Having the Commission add to the requirements independent of the NIST stakeholder process would fragment the requirements development process and potentially cause conflicting overlaps. To the extent such criteria require revision, it should be done through the NIST process in collaboration with technical subject matter experts.

[35] *NPRM* ¶ 40. To the extent the Commission adopts such a requirement, the rule should expressly recognize that a period of zero days support is acceptable, provided that is disclosed. The disclosure should also reflect a manufacturer's reasonable expectations for support, acknowledging that force majeure circumstances may arise that could change the support period.

[36] For example, key questions include: how manufacturers determine which vulnerabilities to patch, how manufacturers ensure patches are secure, with what frequency/process manufacturers commit to patch, etc. 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.

[37] NISTIR 8425 at 9.

To maintain the consistency and integrity of the criteria development process, any additional criteria to which a U.S. Cyber Trust Mark program must align should be developed through the NIST process and incorporated into updated versions of NISTIR 8259 and NISTIR 8425. For example, the U.S. Cyber Trust Mark program itself should not distinguish requirements based on criticality, but rather empower risk management based on the environment in which an IoT product is deployed.[38] Because the horizonal risk of botnets is relatively disconnected from the intended usage of the device, the concept of "high-risk" devices is less about device type (baby monitor, ink jet printer, etc.) and more about secure-by-design and installation considerations.

To the extent the agency wishes to expand the Criteria, the Commission should only identify additional criteria by working with NIST and industry to update the baseline capabilities in NISTIR 8259 and labeling criteria in NISTIR 8425. Similarly, in cases where the federal government determines expert agencies should develop tailored criteria (e.g., directing the Department of Energy to develop criteria for smart meters and power inverters), those agencies should submit that criteria to NIST for incorporation into the unified labeling criteria and related guidance.

C. In Administering the U.S. Cyber Trust Mark Program, the FCC Must Balance the Need for Scalability and Efficiency with the Need to Ensure Consumer/Governmental Confidence in the Integrity of the Label

1. The Cybersecurity Labeling Process Should Remain Distinct From FCC Equipment Authorization

As a general matter, the Commission should foster a streamlined process for implementing the U.S. Cyber Trust Mark and refrain from adding unrelated regulatory steps.

[38] *NPRM* ¶ 27 (seeking comment on whether there are separate criteria that should be considered for higher risk IoT devices or classes of devices).

More specifically, approval via the FCC's equipment authorization rules should not be a prerequisite for achieving the Mark.[39] 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. Additionally, design of marketing materials, packaging, and labeling typically occur months before a manufacturer obtains its FCC equipment authorization. Because the equipment authorization program stands alone and is not designed to address cybersecurity, there is no value in ensuring that equipment authorization is complete before beginning the labeling process for a particular IoT product. Indeed, the Criteria do not include FCC equipment authorization; therefore, making equipment authorization a prerequisite for the Mark is akin to adding an additional criterion.

Manufacturers want to leverage the Mark as a differentiator to help sell IoT devices, but requiring equipment authorization could prevent this. Many companies time the publication of equipment certification on the FCC's website so that it coincides with the public announcement of a product for marketing reasons, for example, to prevent leaks about an innovative device.[40] Such devices could potentially enter the marketplace without the U.S. Cyber Trust Mark, even though those devices would earn the Mark. In addition, tying equipment authorization completion to the completion of the Cyber Trust Mark process will needlessly complicate implementation of the IoT product registry because it would have to be designed such that equipment authorization status would be required as a "trigger" to allow the QR code to display a

[39] *See id.* ¶ 49.

[40] *See* 47 CFR § 2.915(d) ("Grants [of certification] will be from the date of publication on the Commission Web site …. The official copy of the grant shall be maintained on the Commission Web site.").

product that earned the Mark. The Mark and equipment authorization processes should remain distinct from each other.

2. A Tiered and Measured Approach to Accreditation, Eligibility and Enforcement Will Engender Mutually Reinforcing Program Oversight

The U.S. Cyber Trust Mark program should leverage a tiered system to distribute approval and oversight responsibilities. The Commission should approve third-party bodies (or deputize a licensing authority to approve such third parties) responsible for ensuring that products that obtain authorization to use the Mark through their schemes meet program requirements. To the extent the program requires more regular, centralized decision-making or oversight, the Commission may consider leveraging an industry body (perhaps a consortium of scheme owners) to ensure that the program is administered and issues are adjudicated in an effective, objective and timely fashion. CTA's R14 Working Group 6 is developing a Scheme Evaluation Framework for the FCC's consideration to provide an objective, transparent and rigorous process for schemes to demonstrate alignment to the U.S. Cyber Trust Mark requirements (based on NISTIR 8425).[41] Third-party labs should be accredited using industry standards, such as ISO/IEC 17065, ISO/IEC 17025 and other industry guidance.

Regarding industry guidance, the ISO standards only relate to *general* conformity assessment and laboratory processes without being specific to any topic. ISO/IEC 17065 notes that it contains "general criteria for certification bodies operating product, process or service certification schemes."[42] ISO/IEC 17025 specifically addresses laboratory competence, stating

[41] *See* Letter from J. David Grossman, Vice President, Regulatory Affairs, CTA, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 23-239, at 2-3 (Aug. 31, 2023).

[42] *See* International Organization for Standardization, ISO/IEC 17065:2012, Conformity assessment—Requirements for bodies certifying products, processes and services (Sept. 2012), https://www.iso.org/obp/ui/#iso:std:iso-iec:17065:ed-1:v1:en.

that it contains "requirements for laboratories to enable them to demonstrate they operate competently, and are able to generate valid results."[43]

Along with general conformity assessment and laboratory competence, a CyberLAB should also have expertise in the domain of cybersecurity and IoT. CyberLAB technicians will be required to evaluate IoT device capabilities and exercise IoT device functions in the test environment. For example, an IoT device must encrypt data in transit,[44] therefore, technicians in the CyberLAB must have sufficient expertise to verify that transmitted data is encrypted. Consequently, a CyberLAB must employ staff with certain capabilities of such domain expertise. This domain expertise should be validated by a program-designated Domain Accreditor. The Domain Accreditor should be a body of subject matter experts able to set and evaluate professional standards for cybersecurity and IoT. Industry Subject Matter Experts (SMEs) are best positioned to set and evaluate such standards.

The program should prioritize self-assessment and self-approval processes as the structure underlying a self-attestation option to use the Mark. Self-attestation is key to incentivizing manufacturer participation, but CTA recognizes that third-party approval may also have a role to play. If done right, a massive number of IoT devices will seek the U.S. Cyber Trust Mark. Self-attestation will help support the scale, efficiency and cost effectiveness of the program. However, to ensure public confidence and program integrity, the Commission will need to establish appropriate trust mechanisms for approvals obtained by self-assessment. For example, self-attestation should require manufacturers to establish processes for in-house testing.

[43] *See* International Organization for Standardization, ISO/IEC 17025:2017, General requirements for the competence of testing and calibration laboratories (Nov. 2017), https://www.iso.org/obp/ui/#iso:std:iso-iec:17025:ed-3:v1:en.

[44] NISTIR 8425 at 7.

The Commission should establish rules for the supporting documentation required for approval via self-attestation, which could be held on file for a period by the manufacturer. The Commission may choose to incorporate audits into this process as well.

Third-party technical bodies should be responsible for a common level of market oversight. Given the cost and scale of this challenge, the Commission should not undertake market oversight directly, but instead provide clear rules and hold third-party technical bodies (i.e., CyberLABs) accountable for upholding the integrity of the Mark. Consistent with standard industry practices, a third-party technical body should propose an acceptable market surveillance plan in its request for FCC approval. Market surveillance should include random selection of a certain number of products for verification of technical requirements. Market surveillance rules should also require third-party technical bodies to verify to some degree that manufacturers are in compliance with non-technical requirements. Conducting these activities will require substantial staff, time and resources so third-party technical bodies must be allowed to charge fees for their services in executing the program. Competition among third parties approved to implement the labeling program will ensure fees are market based.

CTA agrees that manufacturers should be required to renew U.S. Cyber Trust Mark approvals; however, when and how renewal should occur requires further consideration. Renewal periods may depend on the risk profile of the product. The process will also need to account for variations in product lifecycle and end-of-life procedures. A full re-assessment triggered by every ordinary software update would be overly burdensome and impact the decision to make a software update, including those that mitigate cybersecurity risk. Given the critical importance of security updates post-market, the program should rely on initial assessments, the required documentation of secure-by-design processes as per the NIST Criteria and market surveillance. The program should not require more than an updated filing, in a manner consistent with initial filing rules, when software updates are made.

Products from companies formally identified as posing a national security risk should not be eligible to achieve the U.S. Cyber Trust Mark. The program should observe the same restrictions as the government lists on which they rely for national security-based exclusions. For example, products from companies on the Covered List should be ineligible for the Mark.[45] Manufacturers should formally attest that the IoT product for which they seek the U.S. Cyber Trust Mark is not subject to U.S. government national security restrictions such as those on the Covered List. As the Commission has recognized in other proceedings, such as its implementation of the Secure Equipment Act, the Commission cannot and should not make unilateral decisions regarding national security determinations.[46] To the extent that the U.S. government determines the U.S. Cyber Trust Mark merits a broader set of national security exclusions than existing restrictions such as the Covered List, the Commission should seek guidance from appropriate national security agencies (e.g., FBI, DOJ, NSA, and DOD). In any case, the U.S. Cyber Trust Mark rules should establish clear lists and sources of national security-based exclusions that are straightforward for manufacturers and third-party administrators to implement.

[45] *See NPRM* ¶ 17 (proposing to exclude from the labeling program any such previously authorized "covered" equipment).

[46] *See Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, Report and Order, Order, and Further Notice of Proposed Rulemaking, FCC 22-84, ¶ 19 (rel. Nov. 25, 2022) (citing the Secure Equipment Act; *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Second Report and Order, 35 FCC Rcd 14284 (2020)).

Consistent with longstanding U.S. trade policy, authorized labs based outside the United States should be able to issue the U.S. Cyber Trust Mark, as is the case with similar programs.[47] Under the World Trade Organization Technical Barriers to Trade Agreement, the United States is committed to ensuring "that technical regulations are not prepared, adopted or applied with a view to or with the effect of creating unnecessary obstacles to international trade."[48] Accordingly, "technical regulations shall not be more trade-restrictive than necessary to fulfil a legitimate objective, taking account of the risks non-fulfilment would create."[49] While national security requirements are a legitimate objective, prohibiting all labs outside the United States from participating in the program—including well-respected, accredited test labs based in partner and allied countries—would be far more trade restrictive than necessary to ensure that test labs participating in the U.S. Cyber Trust Mark program are not subject to foreign adversary influence. Such an approach would vastly diminish manufacturers' abilities to select and access evaluation labs, conduct proper risk management and promote competition and diversity in the lab market. It could also hinder the U.S. government's ability to achieve mutual recognition for the program abroad. To the extent the Commission adopts additional measures to vet approved bodies and test labs for the U.S. Cyber Trust Mark program, it should ensure these measures are targeted to address material national security risks.

The Commission should similarly establish a tiered process for enforcing the U.S. Cyber Trust Mark program requirements. FCC-approved CyberLABs should have a process for remediating and/or revoking approvals for products that fall out of compliance with the Mark

[47] *See NPRM* ¶ 26.

[48] World Trade Organization, Agreement on Technical Barriers to Trade, Art. 2.2 (Sept. 19, 2023), https://www.wto.org/english/docs_e/legal_e/17-tbt.pdf.

[49] *Id*.

requirements. The Commission itself should establish a process for revoking the approval of a scheme owner, technical body or test lab that falls out of compliance with the program's rules. For situations where the manufacturer wishes to dispute a failure to attain the Mark or a decision to revoke Mark status, there should be a well-defined appeals process. In cases where a company or organization has made a material misrepresentation to the Commission or one of its approved third-party administrators regarding adherence to the program rules, it may be appropriate to refer the matter to the U.S. Department of Justice.

IV. THE LABEL SHOULD PROVIDE MEANINGFUL ASSURANCE TO CONSUMERS AND LEGAL PROTECTION FOR MANUFACTURERS AND RETAILERS

A. Achieving and Maintaining the Label Should Indicate that an IoT Product/Device is Equipped with "Reasonable Security"

To encourage adoption by manufacturers, the Commission should clarify that IoT products that legitimately achieve and maintain the U.S. Cyber Trust Mark are presumed to have "reasonable" security and that other government actors should recognize it as such. That is, companies that achieve and maintain the Mark in good faith should not be liable for violating laws or regulations that require IoT products to have "reasonable" security. Retailers should also be able to rely on manufacturers' representations regarding the label without fear of being held liable if the product is not in compliance or falls out of compliance.[50] The Commission should expressly encourage other regulatory agencies and legislatures to consider the Mark as an indicator of "reasonable" cybersecurity practices. In particular, the Commission should clarify

[50] In a similar vein, the FCC has determined that service providers may rely on manufacturer reports with respect to hearing aid compatibility ratings. *See Revisions to Reporting Requirements Governing Hearing Aid-Compatible Mobile Handsets*, Report and Order, 33 FCC Rcd 11549 ¶ 21 n.60 (2018) (citing *Improvements to Benchmarks and Related Requirements Governing Hearing Aid-Compatible Mobile Handsets*, Report and Order, 31 FCC Rcd 9336 ¶ 49 (2016).

that the Mark is an indicator of "reasonable" security for the purposes of (i) state laws, (ii) Federal Trade Commission (FTC) enforcement of unfair and deceptive cybersecurity practices and (iii) private litigation.

Executed correctly, the Mark will facilitate a more common understanding of "reasonable" cybersecurity labeling practices to help align emerging state, regulatory and judicial decisions around IoT cybersecurity. A potential patchwork of regulations and laws could create more compliance costs for manufacturers when building innovative products without meaningfully increasing cybersecurity of IoT devices. Already, manufacturers must adhere to state IoT laws—such as in California where IoT products must have reasonable security features—as well as general tort and consumer protection laws.[51] But it is not helpful for these rules to vary in each state, territory and court. Further, companies may face lawsuits even when implementing good security. With respect to IoT devices, the FTC could bring a suit, for example, against a company that allegedly endangers consumers through lax security features or against a company that claims to include reasonable security features in an IoT device but is alleged not to have included such features.[52]

Leveraging NIST's established and credible guidance, as discussed above, would improve the likelihood of other regulatory bodies acknowledging the Mark as "reasonable" because NIST is already seen as a credible arbiter of determining reasonable cybersecurity practices. For example, the California IoT security law includes a provision that a manufacturer of a connected device may elect to satisfy the reasonableness requirement by ensuring the device

[51] *See* Ca. Civ. Code § 1798.91.04.

[52] *See generally* FTC, Privacy and Security Enforcement https://www.ftc.gov/news-events/topics/-protecting-consumer-privacy-security/privacy-security-enforcement (last visited Sept. 15, 2023).

conforms to a NIST conforming labeling scheme,[53] and the FTC also has promoted NIST frameworks.[54] Setting forth clear criteria, aligned with NIST, and enforcing the Mark's integrity will also help establish the Mark as an indicator of "reasonable security."

B. The Commission Should Work with NIST and the State Department to Promote International Alignment and Mutual Recognition

International alignment of cybersecurity labeling requirements and mutual recognition agreements will lower IoT product costs for manufacturers and consumers and encourage widespread and quicker adoption of the Mark by manufacturers. Harmonization of the U.S. Cyber Trust Mark with regulatory and voluntary programs in other countries is an important incentive for participation in this program. Manufacturers seek to "test once, sell everywhere," and while that vision is unlikely to be fully realized, the U.S. must coordinate with like-minded nations and regions where possible to make the program a true success.

Additionally, "consumer IoT" is not the only sector that should be considered from a U.S. government perspective. Accordingly, the Commission should work with the State Department and NIST to coordinate a unified policy approach to international entities maintaining cybersecurity programs.

There are various international fora where the United States should lead in harmonizing global cybersecurity labeling practices and pursue mutual recognition agreements. In particular, the United States should work within the international IEC System for Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE)[55] process to achieve international harmonization/mutual recognition within the applicable portion of the

[53] Ca. Civ. Code § 1798.91.04(c)(1-3).

[54] *See* FTC, *Understanding the NIST Cybersecurity Framework*, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last visited Sept. 30, 2023).

[55] IECEE, About Us, https://www.iecee.org/who-we-are/about-us (last visited Sept. 30, 2023).

Commission's program. Other bilateral and multilateral fora, such as the U.S.-EU Trade and Technology Council may also be helpful, especially for the portions of the program that do not align with IECEE, such as self-attestation, SDOC or industry certification.

The United States can also work directly with specific countries to harmonize criteria and processes for cybersecurity labels. National agencies such as the Cybersecurity Agency of Singapore, the Ministry of Economy, Trade and Industry in Japan, the Korea Internet & Security Agency (KISA) or Directorate-General for Communications Networks, Content and Technology (DG Connect) in the EU may be particularly helpful for manufacturers to have harmonized criteria and processes.

In each of these fora, the State Department, NIST and FCC play a unique role, but should coordinate to advocate for cybersecurity labeling practices that align with the U.S. Cyber Trust Mark Framework. This advocacy should include that the labels be voluntary and flexible, and that regulatory agencies and legislatures should engage in a multi-stakeholder process to incorporate industry-driven best practices.

V. THE COMMISSION SHOULD WORK WITH STAKEHOLDERS TO DESIGN AN EFFICIENT AND EFFECTIVE LABEL THAT MEETS CONSUMERS' NEEDS AND ATTRACTS INDUSTRY PARTICIPATION

A. A Successful IoT labeling Program Relies on Consumer Education

CTA appreciates the Commission's recognition that the success of the U.S. Cyber Trust Mark program will rely on a robust education campaign with effort across the program's stakeholders to promote recognition, brand trust and transparency.[56] The U.S. government should lead this effort, with key focus on driving consumer awareness of the brand and how to interpret

[56] *NPRM* ¶ 53.

the label. The private sector can augment the government's educational campaign through advertising, websites and social media.

The Commission, in consultation with industry experts and consumer advocates, should review NIST's recommended education materials to tailor the plan for the U.S. Cyber Trust Mark. NIST cast a wide net in its guidance regarding an IoT cybersecurity labeling educational campaign. As the FCC launches the U.S. Cyber Trust Mark program, more targeted messaging will more effectively prepare consumers to use the program. Coordination and engagement with retailers in the development of awareness campaigns may increase their impact and likelihood of success. The Commission should also consider how to tailor messaging to other stakeholders, such as retailers that may wish to sell more secure IoT, small- and medium-sized IoT producers who may be unfamiliar with the program, and policymakers interested in IoT security. CTA and its members stand ready to support this effort.

B. QR & Label Design Should be Consumer Friendly and Follow Industry Best Practices

CTA supports the Commission's proposal, consistent with NISTIR 8425, to implement a single, binary label with layered information.[57] This approach will allow consumers to rapidly assess product security at point-of-sale and provide more detailed, up-to-date information to consumers or subject matter experts conducting a more thorough review of a product's capabilities.

CTA advises Mark usage rules where manufacturers place *only* the Mark logo, a QR code or a human-readable URL (matching the QR code data) on the product packaging, or a combination thereof, because any additional "static" information will become outdated and could

[57] *Id.* ¶ 35.

provide incorrect information to consumers.[58] Indeed, additional static information is unnecessary and impractical to implement the just-in-time aspect of education via device label. In most if not all cases, consumers will not be using a QR code absent internet service. Further, standard QR code formats can rarely contain both a usable link *and* a fallback of plain text when there is no internet connection, so the FCC should utilize a QR code that contains a URL rather than plain text when forced to choose between the two approaches. CTA also notes that for longer URLs, use of URL shorteners should be allowed.

In general, the Commission should afford manufacturers as much flexibility as possible in affixing the U.S. Cyber Trust Mark to the packaging of products that have earned the Mark, including the location of the Mark or through e-labeling, so long as variation does not confuse consumers. The U.S. Cyber Trust Mark will offer a marketing distinction for products that achieve it, so manufacturers will have strong incentives to display the Mark in the most accessible manner. These marketing decisions will necessarily vary between the diverse set of IoT products for which manufacturers aim to achieve the Mark and involve myriad considerations, including what space is available on packaging, how customers are accustomed to receiving information from the company, the product's importation and marketing process, and more. The program will benefit from providing flexibility for companies to determine how (or if) to affix the Mark and QR Code on their product packaging—and such flexibility will likely lead to better understanding regarding consumer education and awareness over time.

Finally, the design of the program and the education of consumers should keep to the principle that the manufacturer is only making representations about the cybersecurity status of a product at the time of shipment. That is, that the product has been tested and found to be

[58] *See id*. ¶¶ 38-39.

compliant with an FCC-accredited cybersecurity scheme at the time of manufacturing. Once the product is sold, aspects such as installation and attachment to third-party applications and services are beyond manufacturer control and should not be in the scope of the U.S. Cyber Trust Mark program.

VI. THE NATIONAL PRODUCT REGISTRY SHOULD INFORM CONSUMERS AND MINIMIZE ADMINISTRATIVE BURDENS ON THE FCC AND PROGRAM PARTICIPANTS

CTA supports the use of an internet accessible national IoT registry where the public may access a catalog of devices and/or products that are approved to bear the Mark.[59]

The National Product Registry ("Registry") should be a searchable list of products that have qualified for the program. The Registry should consist of the database, a consumer-accessible website for product search and an input and maintenance interface for manufacturers. Optionally, there may be a need for access (read-only) interfaces suitable to e-commerce websites and systems integrators. The Registry should also support a secure application programming interface (API) for programmatic access over the internet by authorized entities for various purposes.

The central feature of the Registry should be a cloud-based database of the records of qualified products. Authorized third-party entities may post updates (e.g., newly-certified product, or changes in product certification status or details).

The Registry must support a significant number of product model entries over time. In 2022, there were 14.6 billion new IoT connections globally.[60] On launch, the Registry should be able to support: 1 million individual product model entries and 100,000 consumer searches per

[59] *Id.* ¶ 41.

[60] Ericsson, *Ericsson Mobility Report*, at 11 (June 2023), https://www.ericsson.com/49dd9d/assets/local/-reports-papers/mobility-report/documents/2023/ericsson-mobility-report-june-2023.pdf.

day. In addition, the Registry must be designed to scale upwards. As of April 2023, more than 80,000 product models have qualified for ENERGY STAR.[61] The IoT consumer product registry is likely to be significantly larger than ENERGY STAR over time.

A. The Registry's Design Must Enable Consumers to Access Information about the IoT Device with the Mark without Cost and in an Easy-to-Use Manner

An important characteristic of the Mark is that consumers can rely on the QR code to link them to consumer-friendly security information in a familiar format. As of the announcement of the Mark program, the government intends this QR code to link to a page populated with information from the Registry.[62] Some manufacturers have expressed a preference for a QR code that links to their own landing page on their own site, arguing that it is likely to be more consumer oriented than a centralized, government-hosted site. Other companies have expressed a preference for a centralized system where the QR codes all "land" on a common service; a site that pulls up Registry data dynamically and generates a landing page with current information.

It is important to clearly define the way a consumer would use the Registry. The Registry's consumer interface is for checking product cybersecurity status. It is not intended to be a shopping site; detailed search mechanisms and affiliate purchase links are not recommended. For consumers, the interaction is to enter enough information to identify a product model, then receive information about that model's Cyber Trust Mark status. A consumer wanting to search for, e.g., *a smart TV of 65" with slim bezel, UHD and 4 HDMI inputs* would be best served by an e-commerce or brand site. Such sites may indicate products

[61] Environmental Protection Agency, About ENERGY STAR, at 3 (Apr. 2023), https://www.energystar.gov/sites/default/files/2022_Overview_of_Achievements.pdf.

[62] From the White House briefing for the July 18th announcement, "The FCC intends the use a QR code linking to a national registry of certified devices to provide consumers with specific and comparable security information about these smart products." *See* The White House Statements and Releases, *supra* note **Error! Bookmark not defined.**.

qualified for the Mark based on manufacturer's representations or use the Electronic Data Interchange (EDI) mechanism (see below) to support displaying Cyber Trust Mark status in their own results from their more feature-rich consumer interfaces.

Access to the portal should be available at no cost to the consumer/user. Advertising on the platform should not be used to offset the cost. As Registry infrastructure should be the government's responsibility, the use of advertising could be inferred as favoritism by government of one product over another. In addition, given the mechanics of online advertising, it could inadvertently promote an un-Marked product, which would lead to further consumer confusion.

B. The Registry Presents a Good Opportunity to Enable E-Commerce for IoT Devices with the Mark

Retailers should have the option to access Registry information for e-commerce site search results. This may be done in various ways, such as via a RESTful API[63] for immediate results, or via a synchronized database.

An API-based interface is not suitable for high-volume e-commerce sites. An API call per product, per customer-site-view will lead to high infrastructure costs on the Registry side. Retailers do not want a "live" interface dependency for their sites. Also, information about what products are viewed, at what times and in what volumes, is trade secret data that retailers will not be willing to share with outside parties; an API is an attack surface for that threat.

Rather, retailers should be able to cache the Registry database via an EDI solution. The Registry should support exchanging large documents containing the database and periodic

[63] RESTful API techniques are commonly used in web applications, allowing a server to respond to third-party queries over the internet.

updates. API calls may be part of this solution for incidental goals but would not be the main way in which e-commerce sites have access to the Registry.

Finally, as is the case with the ENERGY STAR registry, retailers should have the option to rely on manufacturer's representations to the retailer that a specific product is authorized to bear the Mark such that the Mark may be used in consumer-facing websites, in-store displays, and other promotional materials related to the product. Requiring retailers to refer to the proposed Registry would present a substantial burden and present unworkable challenges in physical retail stores. Instead, the program should keep to the principle that through the Mark the manufacturer is only making representations about the cybersecurity status of a product at the time of shipment, and the Registry can then serve as a tool for consumers to confirm that status and Mark qualification still applies.

C. The Registry Must Support Systems Integrators Use Cases

In this context, Systems Integration (SI) is the practice of bringing together disparate components and ensuring they function well as a whole. SI providers range in size and scale, as does the typical project. Small projects may be smart home installs for, *e.g.*, a few connected cameras, thermostats, and door locks. Larger smart home projects may involve multi-room security systems, smart lawn sprinklers and pool automation. Enterprises use systems integrators for their correspondingly larger projects. The Registry must support these use cases, including three types of SI access:

- Small scale / direct access – In this access type, the small project manager uses the consumer interface described above.

- Intermediate scale / via commercial SI tools – Commercial solutions exist to service SI professionals' needs regarding product search. When an installer needs, e.g., a thermostat and must specify "three wire or four wire?", they may use an application from a vendor who specializes in a database of HVAC/security/convenience components. The SI professional searches that vendor's database through the supplied app; as a result the app vendor requires access to the Registry. This mode of access can be supported by EDI.

- Large scale / EDI – Sufficiently large systems integrator companies may choose to use EDI, described above.

D. Incorporating Search Keys Will Create a More Useful Registry

The Registry database design will require that each product be recorded with information suitable to search. Partitioning into tables of major product categories (such as "Smart TV", "Baby Monitor", etc.) will improve performance. Product categories and per-category search keys will be required. Industry can provide and maintain a list of appropriate search keys.

E. Government Support to Develop and Maintain the Registry is Crucial

Establishing and maintaining the Registry infrastructure is part of the government's responsibility. Use of the Registry should not be fee-based for private sector entities. The Mark is a government-administered program benefiting from significant support in the private sector.

Development and maintenance of the Registry should follow generally accepted best practices in the IT sector for cloud-based data stores, such as regular off-site backup. Cyber Trust Mark approval is a high-profile task that is likely to attract malicious actors. It is critical that the Registry have adequate cybersecurity provisions to prevent unauthorized exfiltration, deletion or modification of data; data-breach incidents could significantly erode confidence in the Program. The Registry should have a cryptographically protected API to allow for internet-based access by authorized users. This API will allow search (read-only) access for some users. Higher privilege users (*e.g.*, admins) will have read/write/edit/delete access for maintenance purposes.

As technical support, the Commission could consider engaging a third party to host and/or manage the registry as establishing and maintaining such a registry will require significant resources and technical capabilities. The FCC seeks comment on whether the Carnegie Melon

University IoT Security Privacy Label (CMU Label) is a good model.[64] The CMU Label has not achieved consensus support from industry; however, CTA's Working Group 7 is reviewing the CMU Label and other proposals to provide a consensus recommendation of the various inputs to the Commission on this question.

VII. CONCLUSION

A public-private collaboration that combines government criteria, industry consensus standards and existing industry assessment and approval processes will meaningfully help consumers to make wise buying choices and encourage device makers to achieve set cybersecurity criteria, reducing risk. 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, Standards & Technology

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

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

October 6, 2023

[64] *NPRM* ¶ 43.