



1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

Via Electronic Filing

October 27, 2026

Marlene H. Dortch, Esq.
Secretary
Federal Communications Commission
45 L Street NE
Washington, DC 20554

Re: *Cybersecurity Labeling for Internet of Things – PS Docket No. 23-239*

Dear Ms. Dortch:

The Consumer Technology Association (CTA®)¹ submits four industry-developed technical standards to support the Federal Communications Commission's (FCC's) implementation of the U.S. Cyber Trust Mark program.² These standards provide practical details on label design, security of wireless protocols, deprecated technologies, and cybersecurity test reporting. Together, they can help promote consistent testing, reduce compliance burdens, and give consumers reliable information about the cybersecurity of connected products.

CTA and its members have long supported efforts to strengthen Internet of Things (IoT) cybersecurity, including work with the National Institute of Standards and Technology (NIST). Building on this experience, CTA has brought together manufacturers, technical alliances, retailers, and consumer advocates through its ANSI-accredited³ standards program to develop technical standards tailored to the U.S. Cyber Trust Mark.

These standards reflect thousands of hours of work by volunteer industry experts and offer practical, consensus-based solutions to support the program's success.

CTA's Commitment to Free Access

CTA is committed to making any of its standards selected for use in the U.S. Cyber

¹ As North America's largest technology trade association, CTA® is the tech sector. Our members are the world's largest innovators—from startups to global brands—helping support more than 17 million American jobs. CTA owns and produces CES®—the most powerful tech event in the world.

² *Cybersecurity Labeling for Internet of Things*, PS Docket No. 23-239, Report and Order and Further Notice of Proposed Rulemaking, FCC 24-26, (March 15, 2024).

³ The American National Standards Institute (ANSI) is a private non-profit organization that coordinates voluntary consensus standards and conformity assessment systems in the United States.

Trust Mark program available to the public at no cost. These standards will be available both as downloadable documents and in online HTML formats. This commitment will help ensure that manufacturers, testing laboratories, and other stakeholders have access to the technical requirements needed to participate in the program.

CTA-2120: Design Requirements for a Label for IoT Devices

CTA-2120 provides technical specifications for the Cyber Trust Mark label, building on the certification mark design established by the FCC.⁴ The standard defines the layout of the mark and accompanying QR code, including printing requirements based on established industry standards.

It also specifies the content and layout of the webpages accessed through the QR code. These include a consumer-friendly page with basic product information and a second page with more detailed technical information. The standard includes a sample HTML implementation and a data model in the form of an open-source JSON schema to support consistent implementation.

By establishing common design and technical requirements, CTA-2120 can help ensure that consumers receive clear, consistent information regardless of the manufacturer or product.

CTA-2120 is available as a free download through the CTA store. CTA is also finalizing an update to reference the latest version of ISO/IEC 15415, with publication of the errata expected in early November 2026.

CTA-2138: Deprecated Technologies

CTA-2138 identifies technologies that established cybersecurity authorities have deprecated because of known security weaknesses or the availability of more secure alternatives.

Rather than independently determining which technologies should be deprecated, CTA-2138 documents decisions made by recognized authorities. Each entry identifies the technology, the responsible authority, its deprecation statement, and a link to the original source.

This approach provides a consistent, transparent reference that can help manufacturers and testing laboratories identify technologies that may not meet the Cyber Trust Mark program's security requirements.

The standard was last updated in July 2025. CTA continues to monitor announcements from relevant technical authorities to identify changes that may warrant future updates.

⁴ See Federal Communications Commission (FCC), *Certification Mark – U.S. Cybersecurity Labeling Program for Smart Devices*, <https://www.fcc.gov/cybersecurity-certification-mark>.

CTA-5500: Cybersecurity Requirements for Connectivity Protocols

CTA-5500 establishes cybersecurity requirements and best practices for common wireless connectivity protocols used in IoT products, including Wi-Fi, Bluetooth, and Matter and more.

Some protocols offer multiple implementation options, not all of which provide the same level of security. CTA-5500 identifies appropriate security configurations and associated testing procedures to support consistent assessments. It also recognizes protocols with security protections built into their design.

CTA developed these requirements in coordination with the organizations responsible for the underlying technologies, including the Wi-Fi Alliance, Bluetooth Special Interest Group, and Connectivity Standards Alliance.

By drawing on the expertise of these organizations, CTA-5500 provides a practical framework for assessing wireless protocol security without creating conflicting or duplicative technical requirements.

CTA-2133: Cyber Trust Mark Data Format

CTA-2133 establishes a common data format for cybersecurity test reports submitted under the Cyber Trust Mark program.

Testing laboratories may use different reporting systems, making it difficult to compare and review results across the program. CTA-2133 addresses this challenge through a standardized JSON data structure that can accommodate Cyber Trust Mark requirements and relevant ISO/IEC 17025 laboratory requirements.

The standard is designed to work alongside existing Cybersecurity Testing Laboratory (CyberLAB) procedures without requiring laboratories to replace their current reporting systems.

A common reporting format can improve consistency, support automated data processing, and reduce administrative burdens for laboratories, manufacturers, and program administrators.

Conclusion

CTA supports the Commission's goal of giving consumers greater confidence in the cybersecurity of connected products. The four standards submitted here reflect substantial industry investment in practical solutions that can help the U.S. Cyber Trust Mark program succeed.

We encourage the Commission, working with the program's Lead Administrator, ioXt Alliance, to consider these standards as it finalizes the technical requirements and procedures needed to implement the program. CTA and its members stand ready to continue working with the Commission to advance a voluntary, industry-supported program that strengthens cybersecurity while promoting innovation and consumer choice.

Respectfully submitted,

/s/ J. David Grossman

J. David Grossman
Vice President, Policy & Regulatory Affairs

/s/ Mike Bergman

Mike Bergman
Vice President, Technology & Standards

/s/ Rachel Nemeth

Rachel Nemeth
Vice President, Regulatory & Government Affairs

Enclosures

1. CTA-2120, *Design Requirements for a Label for IoT Device Cybersecurity*
2. CTA-2133, *Cyber Trust Mark Data Format*
3. CTA-2138, *Deprecated Technologies*
4. CTA-5500, *Cybersecurity for Connectivity Protocols*



Consumer Technology Association, producer of CES®

SUPPLEMENTAL INFORMATION: LINKS TO CTA STANDARDS

Design Requirements for a Label for IoT Device Cybersecurity (CTA-2120)

June 17, 2025

<https://cta-source.github.io/standards-cta-2120/>

Cyber Trust Mark Data Format (CTA-2133)

August 8, 2025

<https://cta-source.github.io/standards-cta-2133/>

Deprecated Technologies (CTA-2138)

August 26, 2025

<https://cta-source.github.io/standards-cta-2138/>

Cybersecurity for Connectivity Protocols (CTA-5500)

October 22, 2026

<https://cta-source.github.io/standards-cta-5500/>