Cooley

FCC Advances US Cyber Trust Mark Program, Labeling and Certification Requirements

November 10, 2026

The Federal Communications Commission (FCC) is taking new steps to implement its US Cyber Trust Mark program for consumer Internet of Things (IoT) products. On October 27, 2026, the FCC released a Public Notice seeking comment on proposed requirements for displaying the Cyber Trust Mark, renewing product certifications and monitoring certified products after they enter the market.

FCC Chairman Brendan Carr also announced that Commissioner Olivia Trusty would lead the program's rollout and implementation. These announcements signal renewed momentum for the program and Trusty has signaled that the Cyber Trust Mark could begin appearing on consumer products within a year. However, the FCC still must finalize its requirements before the program can become operational.

As discussed in our March 2024 client alert, the program will allow eligible consumer IoT products that meet baseline cybersecurity requirements to display the Cyber Trust Mark. The mark will be accompanied by a QR code directing consumers to information about the product's security features. The goal is to help consumers make more informed purchasing decisions and encourage manufacturers to prioritize cybersecurity.

Proposed labeling requirements

The FCC is seeking comment on the design and placement of the Cyber Trust Mark, including how manufacturers should display the label on product packaging and online retail platforms. The FCC proposes adopting labeling recommendations based in part on industry-developed standards. Under the proposal, the physical label would include both the Cyber Trust Mark and a scannable QR code. The FCC is also considering smaller label formats for products with less packaging space.

The FCC seeks comment on how to provide manufacturers with flexibility while maintaining a consistent and recognizable label for consumers. The Public Notice also addresses how the Cyber Trust Mark could appear in online stores, product catalogs and advertising materials. These requirements could be particularly relevant for manufacturers that sell products through third-party retailers.

The FCC also is considering additional information that consumers would be able to access through the QR code. The proposed cybersecurity information page, sometimes called a "cyber nutrition label," would provide information about a product's security features and support period. The FCC proposes requiring disclosure of whether a product has camera, audio or location-tracking capabilities. The FCC also seeks comment on presenting the information in English and Spanish and making it accessible to consumers using assistive technologies.

Certification renewal proposal

The Public Notice also proposes requirements for maintaining certification after a product receives authorization to display the Cyber Trust Mark. Although the program is voluntary, participating manufacturers would have ongoing responsibilities to demonstrate that their products continue to meet applicable cybersecurity standards.

The FCC proposes requiring manufacturers to renew their certifications every three years rather than the five-year period recommended by industry stakeholders. The FCC expressed concern that a longer renewal period might not adequately account for evolving cybersecurity threats. Under the FCC's proposal, manufacturers would need to submit renewal applications at least 90 days before their certifications expire. Cybersecurity Label Administrators (CLAs), which are responsible for reviewing applications and authorizing use of the mark, would have 90 days to complete their evaluations.

These proposals suggest that manufacturers seeking certification may need to plan for continued testing and documentation throughout a product's life cycle for products that remain on the market for extended periods, rather than treating certification as a one-time process.

Ensuring post-market compliance

The FCC is also considering procedures to ensure that products displaying the Cyber Trust Mark continue to comply with program requirements after entering the market. The Public Notice addresses post-market surveillance by CLAs, including product sampling and independent testing. The FCC proposes that surveillance testing be conducted by a recognized CyberLAB or CLA-operated laboratory rather than a manufacturer's in-house laboratory.

The FCC also seeks comment on additional reviews following significant cybersecurity incidents. Under the proposed approach, the FCC could initiate a surveillance evaluation in response to a major cyber event affecting consumer IoT products. The Public Notice further addresses procedures for handling complaints and responding when certified products no longer meet program requirements. Potential consequences could include termination of a product's authorization to display the Cyber Trust Mark and removal of the mark from affected products or marketing materials.

Next steps

The Consumer Technology Association (CTA) and the program's new Lead Administrator (ioXt Alliance) have proposed technical standards for the Cyber Trust Mark and IoT Cybersecurity Labeling Programs. The FCC is expected to seek comment on technical cybersecurity requirements and testing procedures in the coming months.

Manufacturers of eligible consumer products should continue monitoring the proceeding as the FCC develops the program's final requirements. Companies considering participation in the program may want to begin evaluating which products would be appropriate for certification, and whether their existing cybersecurity testing and software support practices would satisfy the proposed requirements.

Comments on the Public Notice will be due 30 days after publication in the Federal Register, with reply comments due 45 days after publication.

If you are interested in submitting comments on this proceeding or have any questions about the US Cyber Trust Mark program and its potential implications, please contact Cooley attorneys Christy Burrow, Henry Wendel, J.G. Harrington and Giselle Valdez.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our legal notices.

Key Contacts

Christy Burrow **Washington, DC**	**cburrow@cooley.com** **+1 202 776 2687**
Henry Wendel Washington, DC	hwendel@cooley.com +1 202 776 2943
J.G. Harrington Washington, DC	jgharrington@cooley.com +1 202 776 2818
Giselle Alexandria Valdez San Diego	gvaldez@cooley.com +1 858 550 6094

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.