ALERT

White House Introduces Cyber Trust Mark Program

The White House has introduced the Cyber Trust Mark program, a voluntary labeling initiative to help consumers easily identify secure Internet of Things (IoT) devices.

By Brian E. Finch, Jeewon K. Serrato, Mark L. Krotoski, Shruti Bhutani Arora, Christine Mastromonaco, Dayo Feyisayo Ajanaku

TAKEAWAYS

- Administered by the Federal Communications Commission, the program requires products to pass cybersecurity tests to earn the distinctive shield logo.
- This program aims to encourage companies to prioritize cybersecurity while giving consumers confidence in their Internet of Things (IoT) products.

01.29.25

Cybersecurity Trust Mark Program: Building Consumer Confidence in Internet of Things (IoT) Security

On January 7, 2025, the White House announced the finalization of its voluntary cybersecurity labeling program for wireless interconnected smart products administered by the Federal Communications Commission (FCC). The White House announcement comes after an 18-month public notice and comment period. The Cyber Trust Mark program seeks to provide consumers with a simple label to assess whether their Internet of Things (IoT) wireless connected devices in their home are cybersecure.

The Cyber Trust Mark program was unanimously approved by FCC Commissioners in March 2024. Our overview of the program is as follows:

- The U.S. Cyber Trust Mark logo will appear on wireless consumer IoT products that meet the program's cybersecurity standards.

- The U.S. Cyber Trust Mark is voluntary, and receipt of the Cyber Trust Mark logo will be granted after independent testing has occurred. The voluntary program will rely on public-private collaboration, with the FCC providing oversight and approved third-party cybersecurity label administrators managing activities, such as evaluating product applications, authorizing use of the label and supporting consumer education.
- Compliance testing will be handled by accredited labs.
- Examples of eligible products may include internet-connected home security cameras, voice-activated shopping devices, smart appliances, fitness trackers, garage door openers and baby monitors.
- Approved products will be authorized to use a distinctive trademarked shield logo on their product.
- The logo will be accompanied by a QR code that consumers can scan, linking to a registry of information with easy-to-understand details about the security of the product, such as the support period for the product and whether software patches and security updates are automatic. Holding of the Cyber Trust Mark logo is contingent upon following the FCC's program requirements.
- The FCC will work with other federal agencies to develop international recognition of the FCC's IoT label and mutual recognition of international labels.

The program is aimed at incentivizing companies to produce more cybersecure devices. Products that have passed a U.S. cybersecurity audit will be allowed to legally display the mark on advertising and packaging.

Early adoption of the Cyber Trust Mark could potentially provide a competitive advantage to companies given increasing concerns about cybersecurity as technology becomes more complex. In reaction to these concerns, the Biden administration stated that "Americans are worried about the rise of criminals remotely hacking into home security systems to unlock doors, or malicious attackers tapping into insecure home cameras to illicitly record conversations."

Possessing the mark could be beneficial as it would signal to consumers that the company stands behind the security of their products.

Similar Cybersecurity Certification Programs and Regulations

Certifications like the Cyber Trust Mark are not new. The concept behind the Cyber Trust Mark initiative is comparable to that of the Energy Star program, which was established to reduce greenhouse gas emissions and make it easy for consumers to identify and purchase energy efficient products. Energy Star provides a label for companies that meet energy efficiency requirements outlined in its product specifications.

Since 2002, the Department of Homeland Security has administered the SAFETY Act program (6 USC §§ 441 – 444). Under the SAFETY Act, any product or service that can be used to deter, defend against, respond to or mitigate cyberattacks is eligible for an award under the SAFETY Act. The SAFETY Act is distinctly different from other voluntary labeling programs, however, in that it grants recipients liability

limitations, ranging from a cap on compensatory damages to the presumption of immediate dismissal of liability claims arising out of or relating to cyberattacks involving the SAFETY Act-approved product or service.

Regulations requiring security of connected devices also exist. In 2020, California's IoT law went into effect, and it requires manufacturers of connected devices (any device or physical object capable of connecting indirectly or directly to the internet or Bluetooth) sold or offered for sale in California to equip the devices with a reasonable security feature or features that must be:

- appropriate to the nature and function of the device;
- appropriate to the information the device may collect, contain or transmit; and,
- designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification or disclosure.

At the federal level, The Consolidated Appropriations Act, 2023, under the Ensuring Cybersecurity of Devices provision, introduced new cybersecurity requirements for medical devices, which took effect on March 29, 2023. In September 2023, the U.S. Food and Drug Administration issued final guidance on Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions that provided recommendations to the industry regarding cybersecurity device design and labeling, along with documentation that they recommend be included in premarket submissions for devices with cybersecurity risks.

How Companies Can Earn Their Cyber Trust Mark Label

The U.S. Cyber Trust Mark programs provide companies with the opportunity to test eligible products against the established cybersecurity criteria from the U.S. National Institute of Standards and Technology. Some of the established criteria include using unique and strong default passwords, software updates, data protection and incident detection capabilities. Manufacturers that meet the eligibility criteria should have their products tested by an accredited and FCC-recognized CyberLab, and then submit an application with supporting documents to one of 11 conditionally approved third-party label administrators for review. These label administrators oversee the evaluation of product applications and authorize use of the label.

The FCC will announce when the program is ready to accept applications.

Benefits of Having a Cyber Trust Mark Label

The Cyber Trust Mark label could instill confidence in consumers that their devices are secure and resistant to unauthorized access. While no company can guarantee that their devices will never be hacked, this program is a step in the right direction to providing a wide range of protections that can be included with a product and make it difficult for unauthorized access to occur.

How Pillsbury Can Help

If your company is seeking to obtain the Cyber Trust Mark, has questions about the SAFETY Act or requires legal services, Pillsbury is available to provide assistance and address any legal or related questions.