Cooley

FCC Issues Framework for Consumer Internet of Things Cybersecurity Program

March 22, 2024

Consistent with an announcement from the Biden-Harris administration in July 2023, the Federal Communications Commission (FCC) has released an order establishing the framework for the new US Cyber Trust Mark program. Under the voluntary program, qualifying consumer Internet of Things (IoT) products can display the new US Cyber Trust Mark logo, indicating that the product meets minimum cybersecurity standards. The logo will be displayed with a QR code that will direct consumers to a database with detailed information about the particular IoT product. The program is intended to help consumers make informed purchasing decisions, differentiate trustworthy products in the marketplace and create incentives for manufacturers to meet higher cybersecurity standards.

Along with the order, the FCC released a further notice of proposed rulemaking seeking comment on whether the FCC should prohibit participation in the US Cyber Trust Mark program when the customer data collected by a product, or the software/software updates for a product, could be sent to or come from a "foreign adversary country" as defined by the US Department of Commerce.

While the order establishes a general outline, the details of the FCC's IoT labeling program will be established in further decisions over the coming months. Based on the timelines established in the order, the new program could be up and running by year-end 2024. (For background information about the US Cyber Trust Mark program, see our August 2023 and September 2023 client alerts.)

Consumer IoT products only

Initially, only consumer-focused wireless – not wired – IoT products will be eligible to receive the US Cyber Trust Mark designation. Medical devices, motor vehicles and motor vehicle equipment, enterprise and industrial products, and communications equipment from certain foreign vendors are specifically excluded from the program. To qualify for the program, a product must be internet-connected and capable of intentionally emitting radio frequency (RF) energy, and it must have at least one network interface, such as Wi-Fi or Bluetooth.

The FCC found that consumers' expectations of security extend to the entire product they purchase. Accordingly, the IoT labeling program will apply to "IoT products" rather than merely to "IoT devices," so that the full functionality of all product components necessary to use the IoT device are considered. Examples of the extra components beyond the IoT device itself include networking/gateway hardware, mobile apps for communicating with the device, and cloud services, data processing and storage. The FCC also said manufacturers will be accountable for any third-party applications used with the device: "[W]here a manufacturer allows third-party apps, for example, to connect to and control their IoT product, such manufacturer is responsible for the security of that connection link and the app[,] if such app resides on the IoT product."

Products that are certified will be permitted to display the US Cyber Trust Mark logo, along with a QR code. The QR code will take consumers to a registry with specific information about the product, including information about how to securely configure the device. The details of which data elements will be included in the registry, and how and where the US Cyber Trust Mark logo and

QR code will be displayed, will be determined in a further proceeding.

Two-step certification process

The FCC has established a two-step process for product certifications. Parties first will submit their products for testing by an accredited lab. Labs will not certify products or issue authorizations – they will conduct the required tests and generate test reports. Each test report will be reviewed by a cybersecurity label administrator (CLA) and, if a report demonstrates that a product complies with the IoT labeling program's requirements, a product will be certified and allowed to display the US Cyber Trust Mark logo.

Labs eligible for certification include independent labs, labs operated in-house by manufacturers, and labs run by CLAs. To be certified, a testing lab must be accredited to ISO/IEC 17025 standards to conduct compliance testing, and it will have to meet specific standards that will be developed by the FCC in further proceedings.

Companies participating in the program will pay fees to the labs and to CLAs. The fees to the CLAs will fund the costs of administering the program. The FCC also will require manufacturers to renew the certifications, but it did not state how frequently renewals will need to be obtained.

Next steps

The FCC will take applications for and appoint a lead CLA to oversee the entire program. The lead CLA, in coordination with stakeholders, will develop and recommend specific testing standards, the design and placement for the US Cyber Trust Mark label, and the consumer education plan. The FCC will review the recommendations and accept public comment before adopting the final requirements. After the details of the program recommended by the lead CLA and approved by the FCC are released, the FCC and/or the lead CLA will open the application process for certifying labs and CLAs.

Parties wanting to have an impact on how the program will be implemented should consider monitoring or participating in the further proceedings that will establish the program's specific requirements. For more information about the US Cyber Trust Mark program and the FCC's implementation of it, please reach out to one of the Cooley lawyers listed below.

Key Contacts

Robert M. McDowell Washington, DC	rmcdowell@cooley.com +1 202 842 7862
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