FCC Set to Adopt Cybersecurity Labeling Program

On March 14, 2024, the FCC is likely to approve an Order that creates a new voluntary cybersecurity labeling program for wireless Internet of Things ("IoT") products. Below, we answer some key questions about the program.

What is the program? The IoT Labeling Program will allow certain connected devices to display an "FCC IoT Label," which indicates U.S. government certification that the product meets minimum cybersecurity standards. The label will include a "Cyber Trust Mark," as well as a QR code that directs consumers to a registry containing specific information about the product.

What products are eligible? The program will generally be available for wireless "IoT Products," which are (1) consumer devices that (2) connect to the internet, (3) can intentionally emit RF energy, and (4) transfer information between the physical and digital worlds, including (5) product components (like a backend, gateway, or mobile app) needed to use the device beyond basic operational features. The program is not available for devices designed for enterprise use, medical devices, or devices produced by entities that appear on certain exclusion lists.

What are the minimum cybersecurity standards? The FCC has not yet established the minimum standards. Under the Order, the FCC's Public Safety and Homeland Security Bureau (PSHSB) must designate a "Lead Administrator" of the program. The Lead Administrator, among other things, will develop specific standards and testing procedures for each class of IoT Products. The NIST Core Baseline standards, discussed in NISTIR 8425, will serve as the foundation for the minimum standards that the Lead Administrator develops. The NIST criteria include the following elements: (1) asset identification; (2) product configuration; (3) data protection; (4) interface access control; (5) software update; (6) cybersecurity state awareness; (7) documentation; (8) information and query reception; (9) information dissemination; and (10) product education and awareness. The Lead Administrator will develop these principles into specific standards that it will recommend to PSHSB. If PSHSB approves the recommendations, the standards will be incorporated by reference into the Commission's rules.

How Can I Participate? To participate in the program, a manufacturer must first obtain a conformity testing report from a private-sector lab that is recognized by the Lead Administrator.[1] Then, the manufacturer must submit an application, including its testing report, to a Cybersecurity Labeling Administrator (CLA) (which the FCC will designate, in addition to the Lead

[1] To be recognized by the Lead Administrator, a lab must be accredited to ISO/IEC 17025 standards by an organization recognized by PSHSB as eligible to perform the accreditation based on ISO/IEC 17011. The Lead Administrator can recognize both manufacturers' in-house labs and certain third-party labs.

Administrator). The CLA will determine whether the application is complete and in compliance with the FCC's rules, then the CLA will approve or reject the application.

What If My Application Is Rejected? An applicant can challenge a rejection by seeking review by the CLA. If the CLA affirms the rejection, applicants can seek review of (1) novel questions of fact, law, or policy from the full Commission or (2) all other questions by PSHSB, which must act within 90 days. Applicants can seek review of PSHSB decisions from the full Commission.

When can I apply? The FCC must complete several administrative steps before the program becomes operational.

1. PSHSB must designate the Lead Administrator. The Order does not specify a deadline for the designation.
2. Within 90 days of designation, the Lead Administrator must propose technical standards and testing procedures, recommend how often manufacturers must renew their applications, and recommend designs for the FCC IoT Label.
3. PSHSB must decide whether to accept the Lead Administrator's proposals and incorporate them by reference into the FCC's rules.
4. The FCC must receive Paperwork Reduction Act approval for requirements imposed on entities seeking to participate.
5. PSHSB will issue a Public Notice explaining the process for seeking authority to use the FCC IoT Label.

What happens after an application is granted? Authority to bear the Cyber Trust Mark will be subject to renewal requirements that the Lead Administrator will develop and propose to the FCC. Further, the FCC has directed CLAs to conduct "post-market surveillance" and random auditing of products that bear the Cyber Trust Mark, and PSHSB will develop procedures for submission of complaints about non-compliant use of the Cyber Trust Mark. For misuse of the Cyber Trust Mark, the FCC will pursue administrative remedies (show cause orders, forfeitures, consent decrees, etc.), as well as other actions such as legal claims of deceptive practices prosecuted through the FTC and legal claims for trademark infringement.

What if my product already bears a cybersecurity label authorized by another country? PSHSB and the FCC Office of International Affairs will work with other federal agencies to develop international recognition of the FCC's IoT label and mutual recognition of other international labels, where appropriate.

* * * *

For more information on HWG LLP, please contact Paul Margie, Sean Lev, Adrienne Fowler, or Walter Anderson.