Skadden

Cybersecurity and Data Privacy Update

March 21, 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Joshua Silverstein
Counsel / Washington, D.C.
202.371.7148
joshua.silverstein@skadden.com

Clare Lilek
Associate / Chicago
312.407.0393
clare.lilek@skadden.com

One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Ave., N.W.
Washington, D.C. 20005
202.371.7000

155 N. Wacker Drive
Chicago, IL 60606
312.407.0700

FCC Approves Voluntary Internet-of-Things Cybersecurity Labeling Program

The Federal Communications Commission (FCC) recently approved a voluntary Internet of Things (IoT) Labeling Program, which allows manufacturers of IoT products to earn the FCC's approval to display a "U.S. Cyber Trust Mark" on products that meet the cybersecurity standards of the IoT Labeling Program. As we noted in an August 2023 *Privacy & Security Update*, the FCC's Labeling Program is part of the Biden administration's National Cyber Strategy and was based on a recommendation made by the U.S. Cyberspace Solarium Commission in its March 2020 report.

Key Points

The Labeling Program aligns with trends in Europe and Asia, which have established or are planning similar IoT programs. Initially the program will be open to manufacturers of wireless consumer IoT products, such as connected or "smart" devices like refrigerators, microwaves, televisions, climate control systems and fitness trackers, but may expand in the future.

While the program is voluntary, the FCC declined industry efforts to include a liability safe harbor, so prospective program participants should consider how the label could be used in litigation in the event of an IoT security incident.

Even IoT manufacturers who decline to participate should consider assessing whether their products meet the Labeling Program requirements, because those requirements may be considered as a potential benchmark for "reasonable security" in litigation and regulatory inquiries.

What is the purpose of the Labeling Program?

The Labeling Program arose from the FCC's recognition that IoT products are essential for everyday life and are susceptible to a wide range of common cybersecurity vulnerabilities. The FCC noted that, based on third-party estimates, around 1.5 billion cyberattacks were launched against IoT devices in the first six months of 2021. The IoT Labeling Program intends to provide consumers assurance regarding the baseline cybersecurity of an wireless IoT product, to help consumers make informed decisions, and to encourage manufacturers to develop IoT products with security-by-design principles.

This sort of voluntary cybersecurity labeling program is gaining global momentum. Singapore already has a Cybersecurity Labeling Scheme and Japan recently announced its intention to work with the U.S. on its own IoT labeling program. And in January of this year, the European Union signed on to an IoT safety label plan in coordination with the U.S.

FCC Approves Voluntary Internet-of-Things Cybersecurity Labeling Program

What can be labeled with the Cyber Trust Mark?

This voluntary program will first encompass wireless consumer IoT products, but may expand in the future.

IoT product is an IoT device and any additional product components (*e.g.*, backend, gateway, mobile app) that are necessary to use the IoT device beyond basic operational features.

An **IoT device**, is an Internet-connected device capable of intentionally emitting radiation frequency energy that has at least one transducer (sensor or actuator) capable of interacting with the physical world, coupled with at least one network interface (*e.g.*, Wi-Fi, Bluetooth) for interfacing with the digital world.

In less technical terms, IoT products are wireless smart devices that have infiltrated many consumers' daily lives, including home security cameras, internet-connected appliances, baby monitors, garage door openers, fitness trackers and voice-activated devices.

The following devices are not eligible for the Labeling Program:

- Medical devices regulated by U.S. Food and Drug Administration (FDA).
- Any communications equipment on the Covered List maintained by the FCC, pursuant to section 2 of the Secure and Trusted Communications Network Act (STNCA), which applies to telecommunications and surveillance equipment made by specified foreign companies.
- Any IoT device produced by an entity identified on the Covered List (*i.e.*, any entity named or any of its subsidiaries or affiliates) as producing "covered" equipment.
- Any device or product from a company named on certain other lists maintained by other federal agencies that represent the findings of a national security review.

Who will administer the Labeling Program?

The FCC will oversee the Labeling Program, but the application review and Cyber Trust Mark authorization will be performed by cybersecurity label administrators (CLAs). A lead administrator will be appointed from the pool of CLAs to act at the facilitator between the CLAs and the FCC. The lead administrator will also be responsible for, among other things, stakeholder outreach, managing complaints about the Labeling Program, and approving the labs authorized to perform conformity testing.

How can manufacturers apply?

Manufacturers have a two-step process for obtaining authority to use the FCC IoT Label, which includes obtaining both:

1. Product testing by an accredited and lead administrator-recognized lab (*e.g.*, CyberLAB, CLA lab, or an in-house lab).
2. Product label certification by a CLA.

For wireless consumer IoT products to be labeled with the Cyber Trust Mark, the IoT product must meet the technical requirements regarding: asset identification; product configuration; data protection; interface access control; software update; and cybersecurity state awareness. The IoT products must also meet the following requirements for IoT product developers, including documentation, information and query reception, information dissemination, and product education and awareness.

Eventually, renewal will be required in order to maintain the Cyber Trust Mark label on the IoT product, which will likely depend on the type of IoT product.

Are there liability concerns?

The FCC declined to include a safe harbor or preempt state law to protect from liability manufacturers that voluntarily apply to receive the Cyber Trust Mark. In the FCC's view, IoT products with the Cyber Trust Mark bear an indicium of reasonableness even if such products are compromised. IoT manufacturers should, however, keep in mind that materials submitted to the Labeling Program could be subject to discovery in consumer protection actions in the event a product is the source of a security incident or the cause of an injury.

IoT manufacturers should also anticipate that the FCC's cybersecurity criteria may emerge as a *de facto* standard and benchmark, much like the frameworks issued by the National Institute of Standards and Technology. It may be prudent, therefore, for IoT manufacturers to consider whether to align their products with the Labeling Program's criteria even if they do not seek the Cyber Trust Mark.