wiley

ALERT

FCC Continues Push to Establish IoT Cyber Trust Mark Program

February 23, 2024

On February 22, 2024, the Federal Communications Commission (FCC or "Commission") released a Public Draft of a *Report and Order* that, if adopted, would establish a voluntary labeling program for Internet of Things (IoT) products, pursuant to which eligible products could be authorized to display the newly created U.S. Cyber Trust Mark to indicate conformance with baseline cybersecurity standards.

The FCC's IoT labeling program is a landmark initiative that, if embraced by the private sector, could have a significant impact on the IoT ecosystem as well as the tech industry more broadly. While Congress has considered IoT security and has adopted mandates for federal agency IoT security, it has not directed the creation of a labeling program for the private sector; however, establishing a cybersecurity labeling effort has been a priority for the White House. Consistent with the White House's goal of seeing products displaying the mark before 2024 is out, this FCC initiative has been rolled out on an accelerated timeline: the Public Draft – slated for consideration at the FCC's March 14 Open Meeting – quickly follows the FCC's original proposal for IoT labels.

While the Public Draft represents an important step for the program, there are many implementation, operational, and legal issues that will need to be rapidly worked through in order to meet this aggressive timetable. This will present numerous additional opportunities for manufacturers and others in the IoT space to participate. If stakeholders want to see a different approach or help refine the details of the program as set forth in the Public Draft, they have time to work with the Commission in *ex parte* filings or meetings. The item will come to a vote at the March Open Meeting.

Authors

Sara M. Baxenberg
Partner
202.719.3755
sbaxenberg@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Joshua S. Turner
Partner
202.719.4807
jturner@wiley.law

Practice Areas

Internet of Things

Telecom, Media & Technology

Background

The White House announced the Cyber Trust Mark program in July 2023 with a kickoff event featuring FCC Chairwoman Rosenworcel and tech industry representatives, among others. Consistent with the White House's expected timeline of getting the program up and running in 2024, the FCC followed in short order with an NPRM in August 2023. After receiving public comment, the agency has now released this Public Draft, which previews the *Report and Order* that will adopt rules to establish the program.

The FCC's Notice of Proposed Rulemaking (NPRM) on an IoT labeling program was very broad and asked an array of questions. Overall, the Public Draft Report and Order would take the program in a direction that is consistent with industry feedback in several respects, such as keeping the program voluntary, leveraging the work of the National Institute of Standards and Technology (NIST) for cybersecurity standards and testing procedures, and promoting "close public-private collaboration," such as relying on third-party certification bodies and program administrators. However, the Public Draft also would adopt measures that were more controversial in the record, including mandating the creation of an IoT product registry (albeit a "pare[d] back" version of what was proposed), requiring the mark to apply at the IoT product level (rather than at the IoT device level), and declining to afford any preemptive effect or meaningful safe harbor for program participants. The Public Draft also would make manufacturers responsible for apps that "reside on" their devices and can be used to "connect to and control" the product, as well as the "connection link" between the product and any controlling apps that do not reside on the device.

While the Public Draft addresses numerous questions posed by the NPRM, the item would leave much more work to do. Casting itself as "provid[ing] the high-level programmatic structure" for the program, the Public Draft would delegate to the Commission's Public Safety and Homeland Security Bureau (PSHSB) and a yet-to-be-selected third-party administrator numerous implementation tasks, including the creation of standards and testing programs, the approval of testing bodies and *additional* third-party program administrators, details of label design and placement, the setup of the IoT registry, and a consumer education campaign – just to name a few.

If adopted at the FCC's March 14 meeting, the new regulations or portions thereof will still need to go through review by the Office of Management and Budget (OMB) under the Paperwork Reduction Act before they can become effective, because they involve information collection by the government. It's possible that this process can be completed in time for products to begin using the mark before the year is out, as the White House intends. But a larger question for the program is whether all of the additional implementation work can be completed in that timeframe.

Below, we provide key context for this latest FCC development, and dive into the details of the Public Draft.

Breaking Down the Public Draft

The Public Draft indicates that the *Report and Order* is intended to "provide the high-level programmatic structure that is reasonably necessary to establish the IoT Labeling Program and create the requirements necessary for oversight by the Commission," but recognizes that "further development ... by the private sector

and other federal agencies" will be required for implementation. ¶ 13. The "high-level structure" set forth in the draft *Report and Order* includes the following key determinations and components:

- **Voluntary program**. The program will remain voluntary, as the Commission agrees with commenters that "willing participation will allow the IoT Labeling Program to be more easily achievable than requiring participation in a novel program." ¶ 11.
- **Definition of "IoT Device."** The Commission intends to adopt its proposed definition of "IoT device" from the NPRM (an FCC-modified version of NIST's definition of the same term): "(1) an Internet-connected device capable of intentionally emitting RF energy that has at least one transducer (sensor or actuator) for interacting directly with the physical world, coupled with (2) at least one network interface (e.g., Wi-Fi, Bluetooth) for interfacing with the digital world." ¶ 16.
- **Definition of "IoT Product."** The FCC also intends to adopt its proposed definition of "IoT product," which is the same as NIST's definition: "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." ¶ 21. A "product component" under the draft rules is a "[c]omponent[] which generally fall[s] into three main types per NISTIR 8425: "specialty networking/gateway hardware (e.g., a hub within the system where the IoT device is used); companion application software (e.g., a mobile app for communicating with the IoT device); and backends (e.g., a cloud service, or multiple services, that may store and/or process data from the IoT device)." Appendix A, Draft § 8.202(j).
- **Certification at the Product Level**. Settling a robust debate in the record, the Public Draft determines that the labeling program will apply at the IoT product level – a step the Commission finds is needed to reduce consumer confusion, "provide consumers the necessary scope to satisfy the basic security expectation of the consumer," and also to "effectuate a discernable increase in the cybersecurity posture of the IoT ecosystem at large." ¶¶ 22, 27. In so doing, the Public Draft rejects industry concerns about the relative immaturity of product-level cybersecurity standards as opposed to standards against which component devices can be tested, which are more fully developed. ¶¶ 24-25.
- **Responsibility for Third-Party Apps**. In response to commenter concerns about IoT product-level certification requiring manufacturers to attest to components outside of their control, the Public Draft sets the following standard for when a manufacturer will be responsible for a third-party app: "where 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." ¶ 27. The Public Draft does not elaborate on what it means for an app to "reside[] on" a product.
- **Exclusion of Enterprise, Wired, and Medical Products**. While the Commission would "not foreclose expansion of the IoT Labeling Program at a later date," the initial iteration will be limited to consumer products and will exclude wired IoT products. ¶¶ 29, 39. The program also will exclude medical devices/products given concurrent Food and Drug Administration (FDA) regulation. ¶ 32.
- **National Security-Based Exclusions**. The Public Draft also would exclude from eligibility for the labeling program entities and products found to pose a national security risk. In particular, the relevant rule

would exclude: equipment identified on the FCC's Covered List, other equipment produced by entities that appear on the Covered List, products produced by entities on the Department of Commerce Entity List or the Department of Defense's List of Chinese Military Companies, and products produced by entities that are precluded from federal procurement. Importantly, this prohibition extends to products produced by entities that do not appear on any of those lists, where the product "contain[s] IoT devices or product components" produced by a barred entity. ¶ 33; *see also* Appendix A, Draft § 8.203(a)(2).

- **Multi-Tiered Program Administration.** The Public Draft would have the Commission take the role of "program owner," charged with overseeing the labeling program. ¶ 41. But the program would be administered by multiple "Cybersecurity Label Administrators" (CLAs), with one CLA appointed "Lead Administrator." Under this scheme, the Lead Administrator would, "in collaboration with stakeholders, [] identify or develop, and recommend to the Commission for approval, the IoT specific standards and testing procedures, ... design and placement of the label[,]" as well as "a consumer education plan." ¶ 42. The Lead Administrator also would process applications for labs seeking to conduct product testing under the program, submit CLAs' post-market surveillance findings, and notify the FCC of consumer complaints (PSHSB would be responsible for "determin[ing] the process for receiving and responding to complaints," ¶ 126). ¶ 52. The CLAs would be authorized to license the Cyber Trust Mark to program applicants, and would be responsible for verifying that the products meet the program's requirements. ¶ 48. CLAs also would be required to ensure compliance with IoT registry obligations, participate in consumer education, and conduct post-market surveillance activities. ¶ 53. Under the Public Draft, PSHSB would evaluate CLA applications and select CLAs and the Lead Administrator, and would have authority to impose additional application criteria for CLAs beyond that listed in the draft rule. ¶ 64; *see also* Appendix A, Draft § 8.219(c). ¶ 59. Entities banned from participation in the program for their products due to inclusion on government national security lists likewise would be precluded from being CLAs. ¶ 60. For-profit entities would be permitted to be CLAs. ¶ 62.
- **Standards and Testing Procedures Based on NIST IoT Core Baseline**. The Public Draft finds that the labeling program should be "base[d] ... on the NISTIR 8425, *Profile of the IoT Core Baseline for Consumer IoT Products*," but determines that the criteria contained in the Core Baseline "are general guidelines that must be further developed into a requirements document (i.e. standards) and corresponding testing procedures, which will demonstrate how the product bearing the FCC IoT Label has met the NIST criteria[.]" ¶¶ 57, 102. The Lead Administrator would be charged with developing and recommending standards and testing procedures in collaboration with stakeholders. ¶ 57. In so doing, the draft directs the Lead Administrator to "evaluate and leverage existing work for efficiency and speed to market where appropriate[,]" and points specifically to NIST's *IoT Product Component Requirements Essay*. ¶¶ 57, 104. The draft notes that the FCC "does not anticipate a single standard would ... apply to *all* consumer IoT products," and recognizes that given that certification will occur at the product level, "there may be multiple standards ... applicable to a single IoT product." ¶ 105. Accordingly, the draft further envisions that different standards "or packages of standards" and testing procedures will be created for "each class of products identified by the working group" convened by the Lead Administrator. ¶ 58. PSHSB would be tasked with evaluating and approving the technical standards and testing procedures developed by the Lead Administrator. *Id*.

- **Multiple Options for Product Testing**. Under the approach outlined in the Public Draft, applicants for the program would be able to conduct the requisite conformance testing for their products at third-party "CyberLABs," CLA-run labs, or in-house labs. ¶ 67. Labs would be required to be ISO/IEC 17025 accredited to qualify, in addition to meeting other criteria set forth by FCC rules. ¶¶ 69, 74. PSHSB would be responsible for identifying additional "specific standards" that labs must meet to gain accreditation under the labeling program. ¶ 67. Just as with CLAs, entities banned from the program for national security reasons would be barred from serving as CyberLABs, but labs would not need to be located in the U.S. ¶¶ 76, 78. As set forth above, the Lead Administrator would be responsible for accrediting and auditing labs for the program. ¶¶ 74-75. CyberLABs would be permitted to charge fees for testing. ¶ 80.
- **Two-Step Process for Getting to Use the IoT Label**. Conformance testing would be necessary but not sufficient for program participation; third-party certification would also be required. A manufacturer seeking authority to use the Cyber Trust Mark would have to follow a two-step process under the Public Draft: "(1) product testing by an accredited and Lead Administrator-recognized lab (e.g., CyberLAB, CLA lab, or an in-house lab) and (2) product label certification by a CLA." ¶ 81. Although the draft finds, relying on "lessons learned in the ENERGY STAR context," that "allowing a path to 'self-attestation' is not appropriate at this time," companies would be permitted to use accredited in-house labs for the testing portion of the process. ¶ 86. When a CLA rejects an application to use the mark, the Public Draft envisions that the aggrieved party would appeal to the CLA, followed by review from the Commission, to be undertaken by PSHSB. ¶¶ 94-95.
- **Layered Label: Trust Mark Plus QR Code**. The Public Draft would adopt the NPRM proposal to "implement a single binary label with layering." ¶ 106. Under this approach, the physical label on the product would include both the Cyber Trust Mark and a scannable code, such as a QR code, that that the consumer can use to obtain more information in a publicly accessible registry. *Id.* As noted above, the Lead Administrator would be charged with recommending standards for label design and placement, to be reviewed and approved by PSHSB. ¶ 110.
- **Decentralized IoT Registry**. The Public Draft would adopt the Commission's proposal to create an "IoT Registry" that the QR code will link to, but opts for a significantly "pare[d] back" version based on feedback in the record. ¶ 114. Under this pared-back approach, instead of a single, centrally maintained database, the program would have a decentralized registry, where each manufacturer would maintain information for their own products, but would display that information in a "uniform way," accessed through a "common API." ¶ 113. The information to be displayed in the registry would include details such as product name, manufacturer name, IoT label authorization date, name of the testing lab and reviewing CLA, information on how to change default passwords and "configure the device securely," and whether the manufacturer maintains a software bill of materials (SBOM). *Id.* The Public Draft rejects the NPRM's proposal to include a real-time list of all known security vulnerabilities, but will require the manufacturer to include "[i]nformation as to whether software updates and patches are automatic and how to access [them] if they are not" as well as the "guaranteed minimum support period for the product," which may be zero but must be disclosed. ¶ 113. PSHSB would have authority to impose additional requirements for the information to be displayed in the registry. ¶¶ 113, 121. PSHSB also would be tasked with issuing a subsequent Public Notice on the implementation of the "

common API," including how the API should be "used" and "structured," and "how manufacturers need to maintain and implement the API in connection with its interactions with registry." ¶ 121. That Public Notice also will deal with other details about the registry, including "how the costs involved in maintaining the registry will be handled." *Id.*

- **Renewal Required; Interval Unknown**. The Public Draft finds that renewal of authority to use the mark should be required, but does not establish a specific interval, instead "task[ing] the Lead Administrator to collaborate with stakeholders and provide recommendations to PSHSB on how often a given class of IoT products must renew their request for authority to bear the FCC IoT Label, which may be dependent on the type of product, and that such a recommendation be submitted in connection with the relevant standards recommendations for an IoT product or class of products." ¶ 124. PSHSB will make determinations on these recommendations and revise the program rules accordingly. ¶ 124.
- **Post-Market Surveillance**. The Public Draft would charge CLAs with conducting post-market surveillance, which would serve as a "principle enforcement mechanism" for the program. ¶ 127.
- **Preemption/Safe Harbors**. In the Public Draft, the FCC rejects calls by commenters to "preempt state law" that could impose liability based on the perceived message conveyed by the mark or that would create a state-specific cybersecurity labeling regime. ¶ 131. Moreover, the FCC would expressly "defer to the states to determine whether approval to use the Cyber Trust Mark" meets any comparable state requirements. *Id.* The draft also rejects calls for the FCC to "implement a legal safe harbor" under federal law for participants in the program such as through a memorandum of understanding with the Federal Trade Commission. *Id.* The Public Draft, however, does "reiterat[e] the Commission's view that achievement of FCC IoT Label is an indicium of reasonableness for entities whose products are compromised despite being approved to use the Cyber Trust Mark." *Id.*
- **International Harmonization**. Noting the "importance of ensuring international recognition of the IoT Labeling Program," the Public Draft would "delegate authority to [PSHSB] and the FCC Office of International Affairs to work with other federal agencies to develop international recognition of the Commission's IoT label and mutual recognition of international labels, where appropriate, as promptly as possible[.]" ¶ 135. In January, White House officials indicated that the U.S. had reached agreement with the European Union (EU) on a "joint roadmap" to ultimately enable reciprocity between the FCC's labeling program and an analogous program in the EU.
- **Consumer Education**. As noted above, the Lead Administrator will be charged with developing a consumer education campaign for the labeling program, in conjunction with stakeholders. ¶ 139. While the Public Draft "envision[s] a Lead Administrator-led" consumer education process, the FCC would for its part "coordinate publicizing the benefits of the IoT Labeling Program with the relevant agencies, including the Department of Homeland Security, CISA, FBI, FTC, the Consumer Product Safety Commission (CPSC), and other industry stakeholders who have indicated a willingness to assist with consumer education." ¶ 141. The item also notes the Commission's belief that "retail and manufacturer involvement in promoting the IoT Labeling Program and the limitations of the IoT Labeling Program are important to ensure widespread recognition of the Cyber Trust Mark in commerce[,]" and points to the National Retail Foundation's "willingness to support consumer education efforts." *Id.*

Next Steps

The item – the substance of which is subject to updates or edits from the Commission – is scheduled for a full Commission vote at the agency's March 14 meeting. Leading up to the meeting, stakeholders have an opportunity to raise issues or concerns about the Public Draft through meetings at the Commission or written filings. However, once the "sunshine period" commences, communications about the item will be prohibited. The sunshine period for the March 14 Commission meeting is expected to begin on March 8.

If the *Report and Order* is adopted, there will be numerous additional opportunities for stakeholder participation as the various directives in the item are implemented. These opportunities will include participation in the Lead Administrator's multistakeholder process to determine recommended standards and testing procedures for the program as well as opportunities to comment on PSHSB public notices on various aspects of program implementation including standards and testing procedures, establishment of the IoT registry, and so forth.

Please contact the authors with questions about the Public Draft, the future program and its interaction with current equipment authorization regulations, or how to advocate for your company's interests as the program is implemented.