Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Cybersecurity Labeling for	)	MB Docket No. 23-239
Internet of Things	)	
	)	
	)	

COMMENTS OF CONSUMER REPORTS
October 6, 2023

Stacey Higginbotham
Justin Brookman
Consumer Reports
1101 17th Street NW, Suite 500
Washington, DC 20036

Consumer Reports appreciates the chance to common on the establishment of a voluntary cybersecurity labeling program. We believe the creation of a U.S. cyber trust mark will benefit consumers by helping them find connected devices they can trust on their home networks and with their data. The label will also benefit employers, retailers, and manufacturers, as well as decrease the attack surface available for those interested in harming the U.S. through cyberattacks.

We answer many of the Commission's specific questions in-line below, but wanted to emphasize the following key foundational principles:

- The label should evaluate the IoT product in its entirety, not as only a hardware device. This is because an IoT product includes the sum of all its parts including the cloud, the app, the networking between the device, and the app, as per the NIST 8425 definition.
- Any device maker should have to commit to a set of robust cybersecurity principles, such as not using default or easily anticipated passwords, a vulnerability disclosure program, and a patching program that include regular security updates, in order to obtain permission to display the mark.
- In order to be able to display the mark, device makers should commit to updating their device using over-the-air updates for a set number of years and disclose this support lifetime on the product's box and at point of purchase. This set minimum support period should be long enough to last the reasonable expected life of the connected product.
- Device makers should securely encrypt device data at rest on the device and in the cloud, and in motion when traversing local and public networks.
- As a condition to display the mark, manufacturers should be required to make a standardized set of disclosures, including the types of sensors inside a device, the data those collect, and who has access to that data, in order to populate a product registry

that can be used to hold manufacturer externally accountable, and that can be distilled into more detailed Layer 2 labels.

- Manufacturers should submit a Software Bill of Materials (SBOM) associated with the connected device and the cloud applications supporting it.

We discuss these criteria and ideas in detail below in response to certain specific questions proposed by this NPRM:

11. We seek comment on whether to focus the program initially on IoT "devices" (as defined in this document) and specifically those wireless devices that intentionally emit radio frequency (RF) energy. We begin by considering NIST's definition of IoT devices. NIST defines IoT devices as those devices that have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth) for interfacing with the digital world. We propose two modifications to the NIST definition for purposes of our labeling program. First, we propose to add "Internet-connected" to our definition because, as NIST observes, a key component of IoT is the usage of standard Internet protocols for functionality, which expose IoT to related security threats and challenges caused by being Internet-connected.Second, because the Commission's relevant statutory authorities recognize the more extensive risks of harmful interference associated with devices that intentionally emit RF energy, we propose to include the premise that an IoT device must be capable of intentionally emitting RF energy. In this respect, we are referring to an IoT device, with a wireless interface, that intentionally uses RF energy to communicate or interact with the physical world. Accordingly, incorporating our modifications, we propose, for purposes of the IoT labeling program, to define an IoT device as: (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. We seek comment on our proposed definition.

For the purposes of this rulemaking, we stress that any IoT product needs to include both the physical device, the cloud infrastructure, and the app. For more on this see our answer to Item 13.

As for the device itself, the definition of "Internet-connected" should be clarified to ensure that wired connected devices such as those that act as hubs for Zigbee and Z-wave devices are included within the scope of the program. The definition should also be clarified to encompass

edge nodes of a connected system, not just the hub device. This is relevant because we have seen hackers attack networks such as Zigbee and Z-Wave networks that are not IP and thus not directly connected to the internet. Through these attacks, hackers have accessed the hub and then moved on to the victim's wireless network.[1]

12. We propose to focus the scope of our program on intentional radiators that generate and emit RF energy by radiation or induction. Such devices – if exploited by a vulnerability – could be manipulated to generate and emit RF energy to cause harmful interference. While we observe that any IoT device may emit RF energy (whether intentionally, incidentally, or unintentionally), in the case of incidental and unintentional radiators, the RF energy emitted because of exploitation may not be enough to be likely to cause harmful interference to radio transmissions. We seek comment on this view. Does this proposed definition unduly limit the devices that should be eligible for participation in the cybersecurity labeling program?

This focus on RF emission seems to unduly limit the scope of the program, by arguing that unless an exploit leads to unusual RF emissions, it might not be considered a threat worthy of addressing with a cybersecurity label. However, many hacks that threaten IoT devices, such as stealing credentials from the cloud or accessing a device using a hard-coded password would have no effect on RF emissions. Additionally, the potential harms associated with a hacked device such as data theft or even a DDoS attack, would have no effect on RF transmission. We propose that the focus should be on connectivity over both wired and wireless networks.

Are there specific unintentional radiators or incidental radiators that should be included in the program, or should they be included generally? Alternatively, should we consider adding these devices to the program at a later date?

There are several attacks on sensors or even attacks that use EMI to duplicate sounds that can lead to a hacker activating a smart speaker. These attacks can lead to misinformation

[1] Paul Wagenseil, "Your Philips Hue Bridge can be hacked through its smart bulbs: What to do" *Tom's Guide* (blog), Accessed October 6, 2023. https://www.tomsguide.com/news/philips-hue-bridge-zigbee-hack

triggering a sensor to take harmful action[2] or a smart speaker to take actions[3], but protecting against these specific RF and EMI attacks is only one narrow category of attacks that should be addressed by the mark program.

We also seek comment on any other ways in which our proposal might be limiting or should otherwise be expanded. For example, would the exclusion of wired-only IoT devices impact the success, usefulness and effectiveness of this labeling program and confuse consumers, rather than adequately informing them on IoT devices with appropriate network security standards?

The program should not exclude wired-only devices. There are plenty of wired-only devices that connect via wired Ethernet or Power over Ethernet (PoE) that should be included in this program. Several popular devices such as the Philips Hue hub, Arlo's camera hubs, and Lutron's Caseta hub require an Ethernet connection to connect to the network. Finally, as we explain in response to question 13, this focus on RF emission and the device itself only protects the physical device, when several exploits of IoT products target the cloud back-end. Examples include grabbing credentials stored improperly in AWS or even employees of a company improperly accessing camera feeds or user data as was the case with iRobot's camera feeds accessed by third-party contractors[4] or Ring's employees in Ukraine[5] accessing consumer videos.

13. To ensure that our program is able to be of greatest value to the consumer, we also seek comment on whether we should focus our cybersecurity labeling program on to IoT "products," rather than IoT devices as defined above. For such purposes we could define an IoT product

---

[2] Jayaraj, Irrai Anbu, Bharanidharan Shanmugam, Sami Azam, and Ganthan Narayana Samy. 2022. "A Systematic Review of Radio Frequency Threats in IoMT" Journal of Sensor and Actuator Networks 11, no. 4: 62. https://doi.org/10.3390/jsan11040062

[3] Zhifei Xu, Runbing Hua, Jack Juang, Shengxuan Xia, Jun Fan, and Chulsoon Hwang. May 2021. "Inaudible Attack on Smart Speakers With Intentional Electromagnetic Interference" IEEE Transactions on Microwave Theory and Techniques 69, no. 5. https://par.nsf.gov/servlets/purl/10313032

[4] Eileen Guo, "A Roomba recorded a woman on the toilet. How did screenshots end up on Facebook?" *MIT Technology Review*, December 19, 2022. https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/

[5] Jon Brodkin, "FTC: Amazon/Ring workers illegally spied on users of home security cameras" *Ars Technica*, Accessed Oct. 6, 2023. https://arstechnica.com/tech-policy/2023/06/ftc-amazon-ring-workers-illegally-spied-on-users-of-home-security-cameras/

consistent with the NIST definition as follows: An IoT device and any additional product components (e.g., backend, gateway, mobile app, etc.) that are necessary to use the IoT device beyond basic operational features. We seek comment on this proposed definition of an IoT product eligible for an IoT label.

We strongly agree that the definition of an IoT device must include all elements of an IoT system, given that attacks on the cloud back end are often much easier and lucrative for a hacker trying to access a bunch of devices for DDoS or ransomware purposes. Much like Willie Sutton, who robbed banks because "that's where the money is," hackers target the cloud because that's where the data is. The FCC also cannot forget the network element of IoT product vulnerability either. Man-in-the-middle attacks are a great way to grab data and credentials if a device doesn't use encryption while transmitting the data from the node to a hub, and from the hub to the cloud. Thus any definition of an IoT product has to include the device, the networking, the cloud, and the data and security processes of the company manufacturing the device, and its contractors. If the labeling programs were only to address the physical device and not other system components, consumers would likely be deceived as to the scope and efficacy of the program.

14. Further, we seek comment on whether a program that addresses products (as opposed to just devices) would be more consumer friendly, as the public may find it easier to understand that the product (as a whole) they are looking to purchase meets the IoT security standards, rather than trying to parse which devices (i.e., parts of the product) meet applicable standards.

An IoT label or mark must encompass and certify all relevant parts of the IoT system, not just the physical device with radio connectivity. The benefit of a connected IoT drive is the sum of its parts, so securing only a few of the parts would cause consumer confusion and even harm. If you're going to sell a device where some of the benefits come from having a cloud connection, an app, and connectivity, then those must also be secured.

Likewise, would limiting the label to devices create confusion with consumers who may not fully understand the label does not apply to the entire product?

Certifying connected devices with the trust mark while failing to look at other elements of an IoT system would absolutely result in consumer confusion. If I purchase a connected light bulb, and get hacked on my social media account or have hackers access my network because the manufacturer improperly stored my password data in their cloud, then the harm is attributable to the manufacturer of the light bulb. Without the device, my data would not have been in the cloud. And if I purchased that device assuming it was secure, that would imply all aspects of it are secure.

If the program only encompasses devices, should we differentiate our labeling in situations where a product contains multiple devices, and some devices are labeled and some are not?

The program should not include only devices. NIST advocates that we can include IoT devices as part of a system of devices; for the system to be secure, all devices in the system must meet the baseline security associated with the trustmark. Other accreditors of IoT devices look to systems as a whole in determining which devices to approve. For example the Connectivity Standards Alliance also provides this assurance with Matter. In cases where a user decides to bring in a non-Matter device, then they are warned during the provisioning process that the device is not part of the Matter ecosystem. So in the case of a security system for example, if the cameras, hubs and alarm have the label but the door and window sensors do not, then the overall system should not be able to use the mark.

If so, how could we make this differentiation without causing consumer confusion?

If everything is sold within a box, then everything in the box should be approved to use the mark. Consumers can add devices to their system that do not have the ability to display the mark, but they should get some kind of notification that adding the non-certified device could weaken the security of the entire system.

How do we mitigate consumer confusion if a device label is used in a common packaging environment?

To avoid confusion, if the device is part of a suite of products sold in a box, such as an alarm system, all of the items in the box should be certified.

15. We also seek comment on whether either definition fully accounts not only for the IoT device or product itself, but also the other components that make the IoT device functional and may be vulnerable to attack. For example, there is a category of IoT devices that do not connect directly to the customer's home Wi-Fi network; instead, they connect to an intermediate communication device (i.e., Wi-Fi Gateway) which connects to the home Wi-Fi network. What are the risks and vulnerabilities inherent in the communication between these types of IoT devices or products and their environment?

In addition to a device, the cloud, the networks between the device, hub, and cloud, the app, the manufacturer's processes, and the supply chain involved in both hardware and software for a connected device are all potentially vulnerable, and require some basic cybersecurity practices. On the networking side, there are documented hacks that affect nodes on a hub, including attacks on Zigbee light bulbs[6], using a backwards compatibility feature of Z-Wave[7] to attack door locks, and there are dozens of smart home devices that rely on proprietary wireless protocols to talk to a hub. When considering the data transmitted from the home to the cloud, concerns over man-in-the-middle attacks, product features that let guests in the home control a device, and other potential vulnerabilities dictate that a secure device encrypt data when it travels from the device to the hub and from the hub to the cloud.

Are there other IoT devices or products that similarly have vulnerabilities that would be outside the scope of our proposed definition?

Medical devices that transfer highly sensitive information and may link back to hospital networks deserve special security considerations as do products that are designed to communicate back to infrastructure such as public electric or water utilities. Today, most electric

[6] Li Jun,Yang Qing "I'm a Newbie and Yet I Can Hack Zigbee" (Talk, Def Con 23, Aug 7, 2015.)
[7] Kayla Matthews "Could this Z-Wave vulnerability put millions of smart home devices at risk?" *Digital Trends* (blog). Accessed October 6, 2023. https://www.digitaltrends.com/home/z-wave-vulnerability/

or water utilities communicate with their own devices, or simply send a message to a device in the home such as a connected thermostat. However, eventually homes are likely to engage in bidirectional communication between utilities and connected devices: for example a leak sensor that can communicate back to the utility that a toilet is constantly running, or a solar inverter communicating back to the grid that it could provide needed power. These communications may pose a threat to the energy grid and should be subject to stricter regulation than this consumer-facing voluntary labeling scheme.

Should such concerns be considered when adopting a definition for devices and/or products that would be eligible for the labeling program? If so, how?

This level of bidirectional communication between a consumer home and a hospital or utility will require an additional layer of security that would require more stringent oversight. Those types of devices should be considered beyond the scope of this label.

16. Finally, we recognize that IoT devices and products have proliferated not only in the non-enterprise space, but also in the workplace from office settings to field settings, from medical settings to industrial settings. As such, we seek comment on whether to focus our IoT labeling program on consumer IoT devices or products intended for consumer use or include "enterprise" devices or products intended for industrial or business use, or to otherwise tailor the scope of devices and products covered by the labeling program based on their usage. If commenters propose that the program include a broader array of devices or products beyond the non-enterprise setting, what additional considerations should we take into account for these products or devices, including the relative sophistication and specific needs of the purchasers of these devices?

We do not think bidirectional communication devices that interact with an enterprise, medical, or utility network should be in the scope of this program.

18. In light of this prohibition, we similarly propose to exclude from the program any communications equipment that now, or in the future, has been placed on the Covered List. We also propose to exclude any IoT device that is produced by an entity on the Covered List as producing "covered" equipment. Furthermore, we propose to exclude from the Commission's labeling program and device or product from a company named on the Department of Commerce's Entity List,42 the Department of Defense' List of Chinese Military Companies43 or

similar lists. The cybersecurity label has the potential to convey important information about a device or product's security. We find it could be harmful to consumers to portray such a message on devices or products made by companies our sister agencies have identified publicly as part of their national security review. We seek comment on this proposal and on other government lists that we should consider. How can the Commission ensure any such proposed exclusion is implemented?

We agree that systems that include components included on the Covered List or similar lists should not be eligible to be included within the FCC's voluntary labeling program. If other expert branches of the federal government have deemed those systems to include known security threats, it would be at best confusing, and at worst misleading, to allow a company to represent itself to consumers as having adequate cybersecurity standards.

Should applicants be required to include a written and signed attestation that the particular equipment for which they seek approval is not "covered" equipment (i.e., is not communications equipment that has been identified and placed on the Commission's Covered List)?

Yes, in order to be considered to use the FCC's trustmark, a company should have to certify that it does not use equipment included on the Covered List or similar lists maintained by the federal government.

Are there other products or categories of products that we should explicitly exclude from the program?

As discussed previously, devices with bidirectional communications to public infrastructure or hospitals should be excluded from the scope of the program. However, in general the agency should be able to apply this label to all kinds of devices as long as inclusion within the labeling scheme does not preclude certain classes of devices being subject to higher levels of cybersecurity criteria by other regulators.

22. Oversight and Management of the Labeling Program. In NIST's White Paper on a cybersecurity labeling program for consumer IoT products, it discussed the need for management and oversight of the overall labeling program. Specifically, it contemplated that there would be one entity (the "labeling scheme owner") that would manage the labeling

program, determine its structure and management, and perform oversight to ensure that the program is functioning consistently in keeping with overall objectives; further, this entity would be responsible for defining the conformity assessment requirements, developing the label and associated information, and conducting consumer outreach and education." We seek comment on the appropriate entity or entities to serve in the oversight and management of the labeling program. Should the Commission be the scheme owner to oversee as well as manage the labeling program?

The FCC should be the scheme owner in terms of managing the program (making sure the accrediting bodies and their standards-setting adjust the program every two years to ensure that it fits with the current standards for cyber security best practices), and using its regulatory and enforcement authority to counteract potential misuse. It also should play a role in consumer education and outreach as it has done with the Broadband Nutrition labels and broadband mapping efforts. However, it should outsource the standards-setting and accreditation to NIST or other accredited standards bodies, which can provide the certification documents to third-party testing labs. The third-party labs should provide the testing, but note that the testing process goes beyond the device and must incorporate aspects of the overall product, including best practices for app development, and the cloud. Other governmental bodies such as the Cybersecurity and Infrastructure Security Agency and the Federal Trade Commission can also support the deployment and administration of the program.

If the Commission takes on the role of overseeing the labeling program, should one or more third-party administrators, as detailed below, manage the tasks identified above or some portion of them?

NIST has already developed a series of IoT cybersecurity best practices and guidelines and was tasked by Congress in the IoT Device Cybersecurity Act of 2020 to develop and maintain cybersecurity standards that will apply to government purchases. President Biden's May 2021 Executive Order that called for the creation of this labeling program also directs NIST to set the criteria for the labeling program. This order led to the creation of the NIST 8425 document that offers a good baseline for a Cybersecurity Trust Mark. While the FCC can add

additional criteria through this rulemaking, there is no need to reinvent the entire standards-setting process.

Or, should one or more third-party administrators be designated as the scheme owner(s), and if so, how should the Commission retain and exercise its oversight responsibilities?

See answers above in response to question 22.

24. If the Commission were to utilize one or more third-party administrator(s), we seek comment on how we should select such administrator(s). What qualifications should a third-party administrator possess, and how should the Commission intake and evaluate applications?

What national security considerations are relevant to such qualifications?

Should a third-party administrator(s) be required to have previous experience administering an IoT product or similar conformity assessment program?

Yes, a third-party administrator should have experience in administering similar conformity assessments in order to effectively certify systems for the cyber mark programs.

Given the diversity in IoT devices and products, would it be preferable for third party administrators to have varying areas of expertise?

If the FCC is going to assign a third-party administrator, it should have or be able to develop an expertise in testing physical devices, cloud conformity, app security and business practices.

What level of control or oversight should the Commission retain, and what level of guidance should be provided?

The Commission should be the primary venue for receiving complaints about counterfeit trust marks or instances where a device maker has lied about their certification qualifications or is otherwise noncompliant with the program's requirements. The FCC should also have a mechanism for holding companies that commit fraud as part of a certification process accountable.

Are there entities in this space that should be considered for this role and, if so, why?

Are there benefits to utilizing multiple third-party administrators versus a single administrator?

If there are multiple administrators, how could the Commission ensure standards are consistently applied across similar devices and avoid conflict among administrators?

How could the Commission reconcile the functionalities of each administrator to avoid conflict?

Are there other attributes or qualities that the Commission should require of an administrator?

For example, should the administrator be required to be a non-profit entity?

Should the administrator establish that it would be neutral and independent, with no conflicts of interest (financial or organizational) on the part of the organization or its officers, directors, employees, contractors, or significant subcontractors?

Should we direct PSHSB, coordinating with the Office of the Managing Director and the Office of Engineering and Technology, to develop and implement a selection or qualifications review process?

27. Applying the Baseline NIST Criteria. We seek comment on the adoption of the NIST's recommended IoT criteria as the basis for the proposed labeling program.56 The NIST IoT criteria are based on product-focused cybersecurity outcomes, rather than specific requirements. NIST contemplates that "the outcome-based approach allows for the flexibility required by a diverse marketplace of IoT products" and the "role of the scheme owner is critical to ensure that supporting evidence demonstrates that the product meets the expected outcomes."57 The NIST criteria include: (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.58 NIST has noted that while the first six of these criteria generally concern certain technical product criteria, the last four concern non-technical product criteria.59

How could NIST's IoT criteria, such as product configuration, interface access control, product education and awareness, data production, asset identification, software updates, cybersecurity state awareness, documentation, information and query reception, etc., be leveraged to inform minimum IoT security requirements and standards in a manner that is suitable for conformity assessments (e.g., for technical-related testing and non-technical verification) in appropriate circumstances, or for self- attestation in others?

Implementation of many of these criteria are probably best served by developing a checklist and asking a manufacturer and the lab to ensure that each item on the checklist is

present. As an example, the Federal Energy Regulatory Commission and the North American Electricity Reliability Corporation (NERC) CIP plans have a checklist of elements that any utility has to fill out to help ensure that the grid is more secure.

There are elements that will require more than a simple yes or no answer, and for those, we suggest a standard data format be used for tracking compliance. This will allow the creation of a database of products and their security qualifications that could be accessed programmatically.

Are there other criteria we should consider?

We recommend the FCC consider requiring reasonable privacy protections as a condition to use the trustmark. There is a link in consumers' minds between the cybersecurity of a device and their privacy. From a consumer perspective, it may be equally intrusive or harmful if data is accessed by a hacker or if the data is willfully sold to data brokers.. Additionally, from a national security perspective it's clear that better privacy practices are essential. For example, data from the Strava fitness app exposed the location of secret U.S. military bases[8]. The military can ban the app and other fitness wearables (or attempt to ban smart speakers in officers' homes[9]), but a better solution is to require reasonable privacy practices from manufacturers of IoT devices, so that consumers who choose a device bearing a trustmark can trust that the company is not collecting or sharing more data than is functionally necessary to operate the device. By ensuring reasonable data minimization as a condition for displaying the trustmark, the FCC will empower consumers to select IoT systems that comprehensively protect their data.

---

[8] Alex Hern, "Fitness tracking app Strava gives away location of secret US army bases." *The Guardian*. Jan. 28, 2018 https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

[9] Doug Olenick, "US Army Apparently Rescinds IoT Device Ban." Gov Info Security (blog) Accessed Oct. 6, 2023 https://www.govinfosecurity.com/us-army-apparently-rescinds-iot-device-ban-a-16788

At the very least, as a condition of receiving the mark, IoT manufacturers should be required to provide transparency by way of standardized information about the types of sensors on an IoT product, what data gets sent to the manufacturer, and how the data from those sensors is shared with third parties. This information could then be included as part of a second layer associated with the trust mark program and ideally would become part of a programmatically accessible database that could be accessed by third parties through an Application Programming Interface (API). The benefits of such a system would allow organizations to easily filter out insecure devices or devices that are inappropriate for use in sensitive settings such as in the homes of high-ranking politicians or military personnel.

Are there separate criteria that should be considered for higher risk IoT devices or classes of devices?

Medical devices, including connected consumer devices such as thermometers or CPAP machines are now covered by their own cybersecurity rules in the Consolidated Appropriations Act of 2023 and the IoT cyber trust mark program should not supersede those rules. Additional commentary on this topic can be found in our answers in response to questions 15 and 16.

28. Standards Development Based on NIST Criteria. We recognize that this conformity assessment program must be based on IoT security standards and testing requirements that the IoT devices and product must satisfy to be eligible to receive and use the label. We propose that the IoT security standards be developed jointly with the industry and other stakeholders. In this regard, there may be a number of expert Standards Development Organizations (SDOs), industry groups and government agencies that have both the technical expertise and other requisite experience to contribute to this task. We seek comment on whether the Commission or an outside entity is in the best position to convene these stakeholders, and to timely develop the more specific detail that would allow the consistent and replicable testing necessary to ensure the outcome based NIST IoT labeling criteria are fulfilled.

The Commission should take on the responsibility of convening these stakeholders to develop the testing and standards in conjunction with NIST.

Would the Federal Advisory Committee Act (FACA)60 limit the Commission's ability to convene these stakeholders?

We seek comment on this proposal.

29. We propose that the IoT security requirements and standards would be developed and implemented through the following process:

- *Collecting information: Conduct research, consult with experts, and review existing standards such as those developed and in use by international organizations.*
- *Establishing requirements: Informed by the new data, develop requirements that will help meet NIST core baseline criteria.*
- *Develop the standard: With the requirements established, the standard can be developed. This will involve creating a document that outlines the requirements in a clear and concise manner and a clear mapping between the standards and the device or product criteria.*
- *Reviewing and improving: Ensure that the standard is comprehensive, clear, and suitable for lab testing.*
- *Implementation: Conduct training, testing, and monitoring to ensure that the requirements are satisfied.*

We seek comment on the scope of this work and on this proposed process. What additional factors should be included or otherwise factored into this process?

Much of this work has already been done with the NIST 8425 document. We also have exceptional standards in the ETSI EN 303 645 recommendations. Translating these recommendations into conformance documents has already been done for ETSI and could be done relatively quickly within NIST. The FCC should focus on the implementation of the label and ensuring that devices that get the label have followed the recommendations.

How can the Commission ensure that the views of small, women- and minority-owned businesses, including small IoT manufacturers, are considered in this process?

Invite small device manufacturers to comment on this NPRM.

Considering the amount of work that the industry, NIST, and international community have already completed in this area, how could this work be leveraged to promote the swift development of standards for IoT cybersecurity labeling?

As we have argued previously, we recommend the Commission rely heavily on the extensive work already done to operationalize established cybersecurity standards such as NIST 8245 and ESTI EN 303 645.

How long might this work take to complete?

We seek comment on the shortest but most thorough path to accomplishing this work and the minimum amount of time it should take to develop the standards. We recognize there are other IoT security standards that are already available and seek comments on whether and why the Commission should consider their adoption.

There are other industry-led IoT security standards, such as IoXT or Matter, but these standards are limited in their cybersecurity criteria and would not cover all areas where an IoT product is vulnerable. Other security frameworks such as the NIST 8425 documents or the ETSI EN303 645 provide a more comprehensive criteria for consumer IoT device security. Finally, I Am The Cavalry provides a useful list of criteria developed by a group of hackers working to build safer products.[10]

Are there standards for particular IoT devices or classes of IoT devices that are already sufficiently mature such that they could be readily – or more quickly – adopted?

See answer above.

Should the program start with those devices or products?

No, products such as those certified by the Matter standard are not yet secure enough to support the label. The ETSI standards form the basis of other cybersecurity labels, and have many necessary elements, but the ETSI standard does not require organizations to log data about a device's performance, nor does it require a manufacturer to provide information about a guaranteed support life for a product, both of which are crucial to ensuring a product stays

[10] I am the Cavalry, IoT Cyber Safety Policy Database, https://docs.google.com/document/d/1E-qJ15WGDe5QzlhnjHVqJgwHWApqA0Ms_SqV-9pc5hI/edit#heading=h.7ltixmwckr36 Accessed on October 6, 2023.

secure, and consumers purchase devices that are up front about their lifetime of security updates.

31. We observe that in other contexts, the Commission periodically incorporates by reference various standards established by standards-setting bodies including, but not limited to, the American National Standards Institute (ANSI), Accredited Standards Committee C63 (ANSC C63), and the International Organization for Standardization; and the International Electrotechnical Commission. As the Commission has noted, use of industry-based standards in this context is intended to ensure the integrity of the measurement data associated with an equipment authorization. We recognize that, in addressing cybersecurity standards, timely adoption and speed are a prime benefit of a multi-stakeholder, industry-led approach, which militate in favor of a more streamlined process than the full Commission- level review described above. Accordingly, we propose if standards are developed by outside bod(ies), that they submit the IoT security standards for acceptance by the Commission prior to utilization for testing and other conformity evaluation. In this regard, we propose to direct PSHSB to place the standards on Public Notice for comment in accordance with the rulemaking requirements of the Administrative Procedure Act and, subsequent to reviewing any comments received, accept the standards as proposed or with amendments as warranted by the record. Is this sufficient, or do commenters believe a Commission-level rulemaking is needed?

The NIST 8425 document creates an excellent starting place for setting the criteria for a certification program and should be used to develop the framework. However, if the Commission does plan to adopt outside standards from third-party frameworks, the criteria in those outside standards should be submitted for public comment before they become part of the labeling program.

Alternatively, could an outside body adopt the standards and attest their conformity with the broader NIST criteria in a manner acceptable to the Commission, without the need for further action by the Commission?

What other streamlined processes might be appropriate for prompt review and validation of IoT security standards?

Other solid cybersecurity criteria can be found in guidance from I Am The Cavalry,[11] elements from the Matter standard, the ETSI 303-645 standard, The CMU IoT Privacy and

[11] *Id.*

Security Label[12], and the UK's Product Security and Telecommunications Infrastructure Act of 2022.

32. Conformity Assessments. We seek comment on the process for assessing conformity of consumer IoT products and devices under the Commission's IoT labeling program. While we expect that third-party assessment (testing and other required assessment via CyberLAB, as discussed above) would provide an avenue for conformity assessment, we propose that other approaches also be considered. For example, NIST describes how different IoT conformity assessment activities could be leveraged to demonstrate that consumer IoT devices conform to technical requirements, either exclusively or in combination. In addition to third-party testing, assessment activities could also include the supplier's declaration of conformity/self-attestation of the consumer IoT device where a statement is issued based on a comprehensive review that an IoT device or product comply with the IoT security standards.64 While the Commission's equipment authorization program has evolved over the years, as currently administered the program includes two procedures for equipment authorizations – certification and Supplier's Declaration of Conformity (SDoC).65 Relevant technical RF-based standards listed in section 2.910 of the Commission's rules are incorporated by reference in Part 2.66 The rules specify the obligations of the "responsible party" (e.g., the manufacturer or importer), including warranting that each unit of equipment marketed under the grant of certification or SDoC is materially identical to the unit that was tested or measured.67 We seek comment on the extent to which any of these same procedures may be appropriate for the IoT labeling program. Are there other alternative procedures that are more suitable for the IoT labeling program context?

The Commission should adopt rules that require a responsible party to attest that the connected product is materially identical to the unit that was previously tested or measured. However, because parts of the IoT product, such as the app, will change over time, elements of an IoT product will not remain materially identical to the tested product. For this reason, the FCC should consider some form of refreshment of the mark to take place every year. Manufacturers could self-attest for the annual refresh of the mark, but the original gathering of information and test should rest with the independent lab.

33. Third-Party Compliance Testing and Assessment. We propose that conformity assessments for IoT devices and products be based on compliance assessment (any testing and other requisite assessment) that includes supporting documentation and data submitted by the

[12] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor. "Specification for CMU IoT Security and Privacy Label." www.iotprivacysecurity.org Accessed on October 6 2023 https://www.iotsecurityprivacy.org/downloads/Privacy_and_Security_Specifications.pdf

manufacturer or importer of the IoT device or product in question to a third-party such as a CyberLAB, and that the third party administrator could authorize the use of the IoT security label only for devices that meet the established IoT security standards. Should all IoT devices or products be required to pursue third party compliance assessment, or are there classes of IoT devices or products that should allow for self- attestation?

There are some IoT products that do not use a mobile app or even store user data in the cloud, such as a smart button. Because these devices only have the capacity to transmit very limited data in a very limited context, they present a lower risk. In these cases, the cost associated with getting a third-party lab to test the device may not be justified considering the cost of the device itself. For these categories of low-risk devices, especially those without an app or the cloud connection, it may be reasonable to allow the manufacturer to self-attest in order to use the mark.

36. We seek comment on where authorized program participants should affix the security IoT label. If the Commission's program addresses devices (rather than products), should it be affixed on each IoT device or on the product packaging?

For companies qualified to display the mark for certain products, we support flexibility in terms of how or where that mark is shown to users, so long as the use of the mark is not deceptive. Manufacturers are likely to have the best sense of where the display of the mark is likely to be impactful in consumer purchasing decisions. The Commission should ensure that the mark covers the entire product, not just the device itself for reasons covered elsewhere in the comment (see supra Questions 11-14). As long as companies are required to make standardized submissions to a product registry that is available online, external validators can help ensure that the mark is not being misused.

Should equipment that includes a user display screen be permitted to display the label on the user display screen rather than on the device itself?

Yes.

Should there be limitations or prescriptions on how companies and third-party resellers can use the mark in advertising or sales displays, products or websites?

If the product has legitimately obtained the mark, we see no problem with manufacturers using the mark in advertising or sales displays. It would help educate consumers about the program and create wider awareness of the mark.

We also seek comment on other approaches with regard to what the label should display and where the label should be placed.

IoT devices can come in very small boxes that in many cases already display several badges such as the Matter logo, Works With Google, Alexa, and HomeKit. Adding an additional mark could create more visual clutter on the package; adding a QR code will stress the design further. However, we are confident that the benefits of prominently displaying the mark to consumers will incentivize manufacturers to make sure the mark is readily noticeable. Manufacturers may have less incentive to make sure the QR code or url link is noticeable, so the FCC should mandate that it is placed in close proximity to the mark itself. These should be readily available on the box itself to allow for easy access to the Layer 2 information contained within the label.

37. Layered Information. We seek comment on the use of a QR code or URL to enable consumers to access more detailed information about the device or product, including specific security information, such as the device manufacturers' level of support, software update history, privacy policy, and similar information. To provide consumers with uniform information and minimize the potential for consumer confusion, we propose that there be a single IoT device or product registry associated with the Commission's IoT cybersecurity labeling program, and that any QR code or URL included with the FCC IoT mark provide a link to the IoT product's specific webpage within this IoT registry. We propose to prohibit any additional QR codes or URLs be placed in connection with the Commission's IoT mark. We believe that this would help ensure the integrity of the Commission's IoT label. If third parties are authorized by the Commission to grant use of the cybersecurity IoT label, should the Commission also permit them to generate and specify the QR code and the URL that can be placed next to the FCC IoT mark and require them to prevent the program participants from affixing other QR codes or URLs next to the FCC mark?

We support a requirement for companies displaying the mark to include in close proximity a QR code and url linking to more detailed Layer 2 information. We also support a

general prohibition on including other urls and QR codes close to the mark in ways that may confuse users. However, we would object to a general prohibition on the use of unrelated QR codes on IoT devices and in IoT packaging. Currently, the use of QR codes is a popular method for providing information to consumers on how to connect an IoT device and get it online. These provisioning QR codes are typically located inside the box with the packaging materials, and often on the device itself. If placed on the outside of the box, the FCC's trust mark, QR code, and url to Layer 2 should be designed to look like a single unit so as to avoid confusing the consumer. If the FCC mark, QR code, and url to Layer 2 are also included inside the box, then they should be on a separate page with some explanatory text about the label and how consumers can get more detailed information over time via the QR code and url.

Should the use of the IoT mark be prohibited without the associated QR code or URL?

Yes, to be effective, the mark must be placed in close proximity next to a means for the consumer or external validator to access the necessary context and more detailed information. This is especially important on the outside of the box or at the point of purchase, so a concerned buyer can assess the cybersecurity information in depth.

What information must a company include if they reference the IoT mark in product listings or descriptions?

The should include the mark itself as well as the url and QR code, along with information indicating that a consumer could get more detailed information about cybersecurity practices through the url or QR code.

What alternative approaches should we consider?

38. QR Code. We propose that the FCC IoT label include a QR code that contains consumer-friendly information that is available without Internet connection in addition to a URL to the device's or product's registry page, which is discussed below. In order to prevent consumer

confusion and allow for easy comparison among devices or products, we also propose that the information contained within the QR code for each certified device or product be uniform and include information that is helpful to non-expert, home users of IoT devices and products. In this way, the label would be able to impact consumer purchasing decisions, which are oftentimes made under time pressure while the consumer is at the store choosing between products. We propose the QR code include a description of the device's security (e.g., easy to understand explanation of what security standards the device meets, and how these standards protect the consumer). We also propose the QR code include a statement that while the label indicates the device or product meets certain cyber security criteria that reduce risk, it does not eliminate risk entirely and the label does not imply product endorsement by the label program and that the consumer is encouraged to visit the product registry linked by the URL provided therein to get the most up-to-date security and other information related to the IoT device or product. We seek comment on this proposal and what additional or other information should be embedded in the QR code to be of benefit to consumers.

The QR code needs to be able to provide the latest, up-to-date information in order to be usable, so we disagree with the suggestion that the QR code provide static information encoded at the point the product is shipped. The information encoded onto a box could be months or even years old when a consumer makes their purchase; directing consumers to rely on that outdated information would likely lead to consumers making decisions based on incorrect — or at the very least — incomplete information. Rather, the QR code or url should direct to a dynamic, updated resource with current information. While this would deprive consumers without connectivity the ability to access detailed information about the product, it is more important that up-to-date information be available to a general audience. The information behind the QR code, in Layer 2 of the framework should include:

- The device name and current firmware version.
- Where it is manufactured, where the data is stored.
- Access control protections that include information about passwords, multi-factor authentication, whether or not the data is encrypted while in motion and at rest (including in the home, app and cloud), and patch policies.

- A support statement saying how long the manufacturer commits to support the product through updates, including security updates.
- A list of sensors on the device and the data they collect.

39. Given the static nature of the information stored in the QR code, we urge commenters to consider the types of information that would be appropriate for consumer decision-making without needing to have the information stored in the QR code updated. Alternatively, the QR code could merely provide a link to the IoT registry page for the device or product in question, discussed below.

We don't believe there should be a static resource that isn't connected as per our answer in Item 38. The QR code should point to the same resource as the url.

40. We propose to require that the manufacturer disclose the guaranteed minimum support period for an IoT device or product, during which the manufacturer commits to identify and patch security vulnerabilities in the product.75 While we recognize the length of such a support period is at the discretion of the manufacturer, and may even be zero, we seek comment on the benefits and drawbacks of requiring a manufacturer to disclose, via the label or associated registry entry, the length of time that an IoT device or product would be supported, and the level of support provided.

We strongly urge that the FCC require that a manufacturer commit to supporting a product for the reasonable lifetime of the product as a condition for using the mark. That period should be clearly specified by the manufacturer to the consumer. Because of the importance of this particular element, the FCC should consider requiring companies to specify the period for which they are committing to support the product in close proximity to the mark whenever the mark is used. This could be phrased "Product supported until at least [date]" or in some other clearly understandable way. However, if the FCC does not require disclosure of support period in proximity to the mark, the minimum support period must be included within standardized disclosures made to the product registry. If the proposed support period is unreasonably short or is less than the reasonably expected lifetime of the product, the FCC should prohibit the manufacturer from using the mark in association with that product.

The manufacturer should not get the mark if they do not plan to update or patch. Otherwise, the mark has no value, because a certified device could become insecure days or weeks later thanks to a newly discovered vulnerability. An IoT product without the ability to receive updates or a plan for updates for a reasonable period of time is an inherently insecure IoT device. Obviously, what constitutes a reasonable support period will be contextual and will differ from product to product. For a video doorbell this might be four years, while a light bulb might get support for 10 years.

Should they also be required to disclose whether all or only critical patches will be supported, the regularity with which such patches are made available, whether they are automatically deployed, or what additional steps a consumer may need to take to remain secure when support ends?

The company should be required to provide more standardized details about its patching strategy as part of an overall vulnerability disclosure program for the product registry. This should include how frequently the company plans to make their patches as well as other details. Patching should occur automatically (ideally when the device tends to not be in use), so as to ensure they get applied.

By default, a company's ability to use the mark should be suspended once it has reached the end of the minimum support period attested to as part of certification. However, the manufacturer should have the ability to extend its support date by making a new attestation; in that case, the company should be allowed to continue to use the mark in association with the product until the end of the new support period.

Should we require the manufacturer to provide notice when that support ends?

Yes, this is accepted practice already in mobile phones, with various software packages, and in industrial IoT equipment. Once a manufacturer stops patching a device it quickly devolves into insecurity, so knowing when that data happens is essential for maintaining a

secure home and for preventing the types of attacks that are the rationale for this entire program. Additionally, this will help consumers feel more comfortable purchasing these products.

If the company has an email address for the user of the product, the company should have an obligation to give reasonable advance notice that the device will cease to be supported as of a certain date. Alternatively, this advance warning could be provided via an app notification (if notifications are allowed) or through an disclosure on the device (if the device has a screen or other interface to provide this information in a manner an ordinary consumer would be likely to understand). The company should also transmit a follow-up notice when the company has ceased support of the device. Depending on the nature of the device, it may still be able to function as a “dumb” device without the additional features associated with internet connectivity. In other cases, connectivity may be so central to the functionality of the device that it may no longer be able to operate safely.

How can we ensure this information is meaningful to consumers?

The mark should not be overburdened with information that a consumer will have difficulty digesting. The mark itself should signify that consumers should be able to trust that the device uses reasonably strong security. At most, the Commission could consider adding one or two other fields to be displayed in association with the mark. One reasonable disclosure to mandate be provided in proximity to the mark would be the reasonable minimum support period to which the company has committed.

More broadly, the government and stakeholders will have to embark on an education campaign to teach people what the mark means. Relatedly, we will have to educate consumers that a connected device requires regular updates over time in order to stay secure, and if the third-party databases are created, that the mark will allow for the creation of services that will help the consumer manage their security.

We seek comment on these options and any alternatives to help provide consumers with necessary, accurate, and timely information.

41. IoT Registry. We propose the use of an IoT registry where the public may access a catalog of devices or products that are approved pursuant to the Commission's IoT labeling program. This IoT registry would be accessible via the Internet and serve as a one-stop reference for the public to understand which products in the market bear the IoT label (e.g., consumers could check the registry before they shop). The IoT registry could contain IoT security-related information that is sortable and searchable by manufacturer or brand, device or product vendor, device or product name, model number, firmware/software build version, and other identifying variables, such as a unique asset identification number. We seek comment on this approach.

Are there any similar product registries that have already been established or that are being initiated, and that might be leveraged for these purposes?

The data specified by CMU's IoT Security and Privacy Label[13] is a good place to start. Consumer Reports is currently consulting with stakeholders to develop a more detailed recommendation of all the fields that a company should have to submit and update over time in order to be considered to display the mark.

Should the Commission consider selecting and overseeing a third-party IoT registry administrator, and if so, how could such an administrator be funded?

Should there be more than one administrator or more than one registry, and if so, how should we ensure that accurate, up to date, and complete information is contained in each of them?

Should it be the same third-party administrator contemplated to manage the other aspects of the labeling program as described herein?

42. The QR code and/or the URL associated with the IoT label would include a link to the IoT registry, which would provide detailed information on the IoT product through the product's webpage within the IoT registry. We seek comment on what information should be included within the IoT registry and associated with the QR codes. If the URL is the sole piece of information associated with the QR code, how should registry information be presented or organized to ensure consumer-friendliness?

CMU's IoT Security and Privacy Label provides an excellent example of the data that should be included in the page accessed via the QR code or url. As for the underlying registry, it

[13] Emami-Naeini, Agarwal, Cranor. "CMU Label"

should include a list of how the manufacturer answers each of the security attestations required to gain the label. Those attestations should be based on the NIST 8425 document. Consumer Reports is currently creating a list of such questions along with the Atlantic Council and others in the industry.

Companies providing data as a condition for receiving permission to use the mark should be required to enter their data in a uniform manner — using the same data format — into a database that consumers, entrepreneurs, and device manufacturers can access programmatically using an Application Programming Interface (API). This enables several security-friendly and consumer-friendly applications. For example, a smart home controller or hub could use the information in the registry to section off devices that are beyond their support date automatically into their own VLAN. Or an employer could build an application for an employee to use to check the types of IoT devices in their home for potential violations of the business' security policies. As smart home devices become more common, to ensure their security, we will need some way to automatically manage them.

43. We propose that, among other information, the IoT registry might provide the following information for each approved device or product: 1) how to operate the device securely (e.g., basic cyber hygiene to include changing default passwords) and, if applicable, what level of security the device or product has achieved; 2) whether the product's security settings are protected against unauthorized changes, including disabling its security; 3) where the device was manufactured; and 4) when the registry information for the device was last updated. What other information should be included?

It should include the following:

- A support life for the product
- Patching protocols
- Data encryption information (for example, whether it's encrypted at rest and in motion at all locations)
- What geographic region data gets stored in

- Sensors included in the device and the data they collect
- What data gets shared with third parties
- Whether the manufacturer has good cloud cyber hygiene, such as storing data in an excerpted format, has logging for employee access and device access to data, makes sure only authorized employees have access to data, etc.)
- Instruction for deleting the device from the network and relevant account information in the cloud
- A link to a software bill of materials (SBOM), or even better, the SBOM itself in a machine-readable format.

Would the information included in the CMU IoT Security and Privacy Label (CMU Label) be an appropriate model for each IoT product's listing provided within the IoT registry?76

The data specified by CMU's IoT Security and Privacy Label[14] is a good place to start.

CMU Labels are divided into three major sections: 1) security mechanisms, 2) data practices, and 3) more information, with various data fields under these sections (e.g., security updates, access control, sensor type, privacy policy, manufacturer contact information, and platform compatibility).77 CMU Labels often link to external sites, such as manufacturers' websites, to provide more detailed information. Would linking to external websites, over which the Commission would have no oversight or control, be appropriate for the Commission's IoT labeling program and the IoT registry?

The FCC's registry should not link to other sites — allowing companies to provide data through hyperlinks would be too confusing for consumers or even security researchers and would defeat the purpose of a centralized registry. Rather, the information should be pulled into the more detailed label or into a programmatic database of relevant security information.

How could we ensure the content of the information provided in the external links is accurate and up-to-date?

Manufacturers should be required to recertify their practices each year or to provide updates to the registry in the event of a material change in their behaviors.

[14] Emami-Naeini, Agarwal, Cranor. "CMU Label"

Are there additional exemplary labels that the Commission should consider?

What other additional details should be disclosed to inform consumers of cybersecurity risks underlying the IoT product?

See answer to the first question of point 43.

What details can potentially be omitted?

How can the Commission otherwise ensure the information provided in the IoT registry is meaningful and understandable by consumers?

44. We further ask whether such IoT registry might also be used by retailers to assist them with choosing products that carry the IoT label for sale in their stores and whether retailers may use the registry to confirm that the products that they market legitimately bear the FCC's IoT label. If so, should the registry maintain different sets of information for general consumers and retailers?

We think the right way to think about this is that there is a layer of information delivered in a consumer-friendly format (Layer 2) and a layer of information stored in the programmatic database that is accessible by third parties (the IoT product registry). Retailers are sophisticated enough that they could use the programmatic database to stock products they believe are secure. Plus, the programmatic nature of the database could make it easy for retailers to sort products by specific features as a service to consumers. Retailers would also likely want to sort by support date to ensure they are stocking products that are still supported.

What additional information would retailers want to see but is not relevant to general consumers?

45. Updating Information. We seek comment on how to ensure consumers are not misled by the meaning of the IoT label and can obtain up-to-date information about their device or product. Unlike other labeling programs, such as the Commission's Broadband Consumer Label,78 or the ENERGY STAR label,79 the Commission's labeling program addresses cybersecurity risk, which is constantly changing and requires constant updating. For example, if a new vulnerability is discovered, the product would remain unsecure until that newly discovered vulnerability is patched. We propose that consumers be made aware of any vulnerabilities or updated product information through the IoT registry. That way, once the product's webpage within the IoT

product registry is updated to indicate that the authorization to use the mark is outdated, and/or the device is no longer maintained/updated, the consumer can understand this information by accessing the webpage using the QR code and/or the URL provided next to the FCC IoT label.

Should we impose a duty on manufacturers or importers of the IoT devices and products to notify the IoT registry operator when they become aware of an unpatched vulnerability that poses security risks to their IoT devices and products?

Manufacturers should have some form of published vulnerability disclosure program, so when researchers notify the connected product maker about a potential vulnerability, the researcher knows what to expect. That program should follow current best practices, such as committing to not suing researchers reporting a vulnerability in good faith, and having a set time frame for addressing the vulnerability.

After assessing the vulnerability there should be a reasonable time frame for a company to notify consumers and then patch it. However, that reasonable time frame should be relatively quick, such as the rules newly adopted by the SEC[15] forcing companies affected by a cyber incident to notify investors within four business days unless the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing. The SEC rules refer to an actual cyber incident, as opposed to knowledge of a vulnerability, but once a vulnerability is exposed, the potential for it to become an incident is high. Any device that has a security certification needs to have policies in place to ensure a rapid response to disclosed vulnerabilities, and if such a program doesn't exist, the consumer should be proactively notified, so they can take the device off their network or quarantine it.

Are there other events that should trigger IoT product manufacturers or importers to notify the registry operator that their IoT registry device or product page should be updated?

---

[15] "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies" U.S. Securities and Exchange Commission. Accessed on October 6, 2023. https://www.sec.gov/news/press-release/2023-139

Companies should be required to update the database when a device is affected by a critical vulnerability, especially one that allows for a remote-exploit, when a company experiences a data breach in the cloud, and when the company stops supporting or prolongs the support period for a product with regular security updates.

46. We seek comment on these proposals, and on any other ways to ensure consumers have up-to-date information regarding IoT devices or products labeled under the program, as well as have an understanding that the FCC cybersecurity label is not a guarantee against all cybersecurity threats.

What additional information might be warranted to help minimize the potential for customer confusion?

This is where the programmatic database containing up-to-date device information comes into play. This is the IoT product registry. With such a tool, accessed by third-parties via an API, existing and new companies can build services that help manage a consumers' IoT device network without requiring the consumer to become an expert or a CISO for their own home. For example, broadband providers might build a security service into their routers that automatically quarantines a device when the database gets an update indicating a critical vulnerability. This leaves the cybersecurity policy management to experts who can handle the complex, and ever-changing security environment on behalf of consumers. To ensure competition in this sector, multiple types of companies should have access to the registered product database unless there is a compelling security reason they should not. This allows multiple services and products to flourish based on the needs of the end consumer.

47. Application/Renewal. We propose that IoT label applicants file for renewal each year, together with supporting evidence that the products still meet the FCC's IoT requirements, as tested and administered by the CyberLABs or as self-attested. In this regard, we seek to ensure consumers have up- to-date information regarding the participating device or product, and to address end-of-life issues for devices previously approved, but that no longer warrant continued authorization to use the label. Should the label include the specific date, or the year, the label was awarded to help notify consumers how fresh the authorization is?

The label and registry should include the date the mark was awarded as well as the date of any subsequent recertifications.

Should the FCC IoT labels on the device or product have an expiration date? How do we ensure consumers are aware of when a device with an FCC IoT label is no longer maintained and/or updated by manufacturers, and may no longer meet up-to-date cybersecurity requirements?

The label should expire when the end-of-support date hits as covered in our answer to Item 40.

48. We seek comment on this proposal to employ a renewal process. Should the Commission consider other timeframes on a shorter or longer basis?

The device should certify annually and manufacturers should update the database if there are any material changes to their cybersecurity practices.

Should there be an event in the product's life-cycle or a security event that should trigger the applicant to file for an early renewal?

When an IoT product maker gets acquired or merges with a new company, it should trigger a re-certification, even if only through self-attestation. When a company buys the intellectual property of another IoT manufacturer out of bankruptcy, the new owner should go through a self-attestation process with regard to IoT devices affected by the purchase.

If the manufacturer decides to end support for a connected product, it should update the IoT product registry that can be accessed via APIs. Companies should not be permitted to end support before the end of the minimum support period attested to as part of certification. However, if a company goes bankrupt and no longer will be supporting the product before the end of the minimum period, it could update the database to reflect that fact. Finally, any time a manufacturer wants to end support for security updates or deprecate the product so it can no longer be used, it should try to contact the consumer separately.

When would such an event trigger early renewal, versus filing updated information with the program administrator and updating the IoT registry?

See answer above.

Similarly, are there incidents or developments that might warrant the removal of the IoT cybersecurity label, and what might those circumstances be?

If the acquirer of an IoT product (through M&A or through an asset sale) fails to recertify, the mark should be revoked. If a company fails to update its annual recertification, the mark should be revoked. If a company fails to implement a patch in a timely manner the mark should be revoked. If a company is found to have included material false information on its certification process, the mark should be revoked.

Additionally if the manufacturer makes changes with regards to shortening the minimum supported lifetime of the product, it should trigger some kind of notice to the consumer. Reduction of support should result in revocation of the label in addition to enforcement by the Commission for failure to abide by commitments made as a condition for displaying the mark. Finally, if a manufacturer wants to end support for security updates or deprecate the product so it can no longer be used, it should try to contact the consumer, and the label should be revoked.

After the IoT device or product is authorized for the first time, what supporting documents should the program participants provide to validate and renew their authorization to use the label?

The focus should be on providing documentation in a standardized, machine-readable format.

Must it be retested annually?

The manufacturers can self-attest annually after the first outside test, as long as the FCC or its agent is conducting random audits and the results of the self-attestation are available in the IoT registry that is accessible by third parties.

How should the IoT registry reflect that an authorization to use the label is out of date?

If a label is out of date, the device can no longer be considered secure, so the label should be revoked with such revocation being featured prominently in the registry.

49. We also seek comment on the interplay between the proposed IoT cybersecurity labeling program and our current equipment authorization rules. Given that the review process for the proposed program will likely not be administered in the same manner, and by the same entities, as are involved in our equipment authorization program, we propose that they generally operate in a distinct manner. However, given that equipment subject to the requirements of our equipment authorization rules must satisfy those rules before they can be manufactured and sold in the United States, we propose that approval be granted under the cybersecurity labeling program only after any applicable requirements of the equipment authorization rules have been satisfied for the relevant device or product. We seek comment on these proposals and on any other ways in which we should address the potential interplay between the proposed IoT cybersecurity labeling program and our current equipment authorization rules.

We support the FCC's proposals with regard to bifurcation and sequencing. It is also possible that over time existing TCBs will develop the expertise to bestow the label, and thus, the certifications could run in parallel.

51. Investigation, Disqualification, and Enforcement. Ensuring that the label remains a trusted and valuable resource to purchasers requires that the integrity of the devices and products bearing the label is maintained. As such, we seek comment on how to enforce the labeling program requirements.

To the extent that non-Commission entities are better situated to perform, and receive approval to perform, certain functions, should they also be required to conduct a certain number of random audits of the certified IoT devices and products to confirm that they are in compliance?

Periodic audits should play a role in supplementing initial testing and self-attestation. Third-party audits by TCBs are one option. We would also like to see a process by which third parties such as hackers, teardown experts, consumer complaints, and others can audit these devices and send their concerns to the FCC. Mandating that companies supply standardized information fields to the product registry will help external validators hold manufacturers accountable.

Are there types of market surveillance that should be conducted, and by whom?

See answer above.

Should we allow consumer or third-party complaints?

Of course.

Should the Commission or other entities accept and process such complaints?

The Commission should be the central repository for complaints, though it could then assign partner organizations to investigate or otherwise follow up as appropriate.

What should the Commission's role be in audit and oversight?

The FCC should require random audits of devices to ensure that they are deserving of the mark, and keeping up with the certification renewal process. The FCC should also ensure that third parties have the ability to file complaints when they find companies who are knowingly or unknowingly not following the appropriate criteria for a device that has achieved the trust mark. And most importantly the FCC should zealously enforce against violations of the mark and transparency programs to ensure that companies are not able to promote their products with the mark if they are not living up to the requisite commitments for doing so.

For any non-compliance, we could rely on a combination of enforcement procedures such as administrative remedies under the Communications Act (e.g., show cause orders, revocation proceedings, forfeitures, consent decrees, cease and desist orders,83 and penalties84) or civil litigation for breach of contract or trademark infringement, in which the Department of Justice (DOJ) would participate.85 As noted above, we also seek comment on what, if any, additional measures are necessary to ensure that the Commission is effectively controlling use of the certification mark for purposes of trademark law.

What enforcement measures would be appropriate for firms that falsely put the IoT certification mark or label on their products?

If a company puts a false label on an IoT product or fails to live up to its commitments for using the label, the FCC should be able to revoke, suspend, or limit the company's ability to use

the label for any product prospectively, obtain injunctive relief against the company — including the cessation of sales of packages with misleading labels — and be able to impose substantial deterrent fines on the manufacturer.

How would it be enforced if firms are outside of the United States?

The FCC should have the same legal powers as it has over domestic companies if the companies are knowingly putting IoT devices into the stream of United States commerce. In practice it may be more difficult to enforce relief against such companies, so it may be necessary to obtain additional injunctive relief from platforms that make such products available to American consumers.

In the more contractual context of the ENERGY STAR program, EPA has set out certain Disqualification Procedures that it would apply if a product fails third-party verification testing, or if it fails subsequent Department of Energy (DOE) appliance testing or in the event of product nonconformity. In particular, this process gives the ENERGY STAR Partner notice and an opportunity to dispute the assessment with EPA before a formal disqualification decision is made. The Disqualification Procedures specify certain steps that ENERGY STAR Partners must take in the event of a disqualification (e.g., removing references to ENERGY STAR in the product labeling, marketing, etc.). Should we adopt a similar disqualification procedure under our rules?

The trust mark should be revocable, and the agency can certainly oversee a dispute process. There is a strong case for letting the FCC revoke the use of the trust mark upon a *prima facie* showing of misuse before a full adjudication of the merits of the FCC's case. At the very least, when the FCC has initiated a proceeding to revoke the label,that information must be communicated to the IoT registered product database. Because the security of a home, or even a nation, is only as good as its weakest link, the risk of letting consumers buy or retailers stock an item during what might become a months-long dispute process is too high to delay any transparency into enforcement until a formal resolution.

What enforcement measures would be appropriate in addition to revoking authorization to use the IoT label?

What procedures or consequences should apply where a device or product was certified under one set of standards but is not capable of meeting a new or updated standard adopted later?

How should the participants address the products that have the IoT security labels affixed to their products when their products become non-compliant?

If an applicant is denied authority to use the Commission's IoT label, should they be able to appeal that decision?

It is reasonable to create some sort of process by which a denied applicant can appeal a decision with new information that addresses the reason the product did not get the label in the first place. However, the Commission has limited resources, so the process must be structured such that better resourced companies cannot abuse the process to coerce the Commission into allowing a company to use the mark in scenarios where they have not materially met the program's substantive requirements.

We also seek comment on any recordkeeping and audit requirements for compliance review purposes.

52. Conversely, where a program participant has received authorization to utilize the Commission's IoT Label and has appropriately maintained the device's security measures, does this represent an indicium of reasonableness that might serve as a defense or safe harbor against liability for damages resulting from a cyber incident, e.g., data breach, denial of service, malware?

Data breach reporting tends to be strict liability — if a breach occurs, companies are obligated to report to both regulators and affected consumers regardless of fault or relative culpability. As such, compliance with the FCC's labeling program should not obviate the company's reporting obligations in the event of a breach.

In the event of an action against a company for inadequate security practices, participation in and full adherence to the requirements of the FCC labeling scheme would obviously be relevant to any finder of fact. However, we are not convinced that a formal safe

harbor program is necessary. First, FCC guidance is not legally binding on other jurisdictions' security laws or other regulators' interpretations thereof, and the FCC lacks the legal authority to assert its views in legal proceedings interpreting other security laws. Second, approval to use the mark is not necessarily dispositive of good security in practice. A company could self-attest to strong security practices and then subsequently fail to live up to those obligations. Finally, while approval to use the mark paired with demonstrated compliance with the FCC's standards is likely to be indicative of reasonable security measures, there will be in any case a substantial burden on companies to demonstrate its compliance. Whether the FCC articulates an explicit safe harbor or not, it will still be incumbent upon the company to prove that it was substantially in compliance with the program's requirements. As such, a safe harbor would mean little in practice, as the company would in any case be required to prove that it had performed all the requisite elements of a robust security program.

While we clarify that we do not intend at this time for the labeling program in and of itself to preempt otherwise existing law, are there other affirmative measures that the Commission should consider adopting that should be afforded to devices that have achieved and maintained a Commission IoT security label?

55. Integrity of the National Government-based IoT Cybersecurity Label. We seek comment on ways to avoid consumer confusion between the government-based IoT cybersecurity label and existing and future IoT cybersecurity labeling schemes such as UL and IoT Security Trust Mark.

What features and assurances can the Commission's label provide to improve customer awareness of the security of a given IoT device?

Layer 2 of the label should provide a glossary of security terms and plain English explanation of why each element included in the registry matters.

Alternatively, should the FCC label act as an aggregator for other labeling programs ensuring that these programs meet the IoT security standards in addition to any wider or sector specific security needs the scheme owners feel necessary.

The FCC has limited capacity to force other labeling schemes to conform to its criteria, and it should not weaken its own program simply to achieve harmonization with industry programs. If other label programs want to adhere to the standards criteria for the trust mark, that would be a positive development for industry and consumers, but broad conformity should not be a requirement for deployment of the Commission's program.

What about other labeling programs in other countries?

The FCC has limited capacity to force other labeling schemes to conform to its criteria, and it should not weaken its own program simply to achieve harmonization with other national programs. If other label programs want to adhere to the standards criteria for the Trust Mark, that would be a positive development for industry and consumers, but broad conformity should not be a requirement for deployment of the Commission's program.

How should the Commission coordinate and engage with other international bodies maintaining labeling programs to develop recognition of the Commission's IoT Label, and where appropriate, mutual recognition of those international labels?

While mutual recognition programs can harmonize conflicting or adjacent security standards for industry, we would strongly object to the Commission meaningfully weakening its program simply to achieve conformity with other programs. Any mutual recognition should only occur when the other program to be recognized has standards as stringent or more stringent than the FCC's trust mark program.

Our proposal seeks to implement this program for devices or products for sale in the United States. What steps, if any, should we take to ensure the FCC label is not mistaken for compliance with IoT security or RF-emission standards in other countries?

56. Accessibility. The Commission emphasizes its continued commitment to ensuring that the labeling program is accessible and usable by individuals with disabilities. With respect to the Commission's Broadband Consumer Label, in 2022, the Commission noted that the Consumer Advisory Committee (CAC) determined that participating providers can best ensure accessibility

to printed and online information by relying on well-established legal requirements included in the Americans with Disabilities Act and by following the guidance developed by the Web Accessibility Initiative.93 We seek comment on whether relying on these guidelines provides the best likelihood of ensuring that consumers with disabilities will be able to access necessary information about their IoT devices or products. We seek comment on how best to ensure that any adopted IoT cybersecurity label is accessible to persons with disabilities.

This is an important aspect of the label, since many connected devices are commonly used by those with various disabilities to make their lives easier. Thus, creating a label that they can access is especially important. For in-store purchases, a label should include a tactile QR code indicator, which is a sticker that contains a tactile square to help the blind and low-vision (BLV) community locate the QR code, and for online purchases the registry should include, compliant with the Web Content Accessibility Guidelines (AA Standards), the availability of multilingual translation for the registry system, and more detailed highlights for assistive smart devices. Material designed for the label should be written for an 8th grade reading level and should not presume any familiarity with the details of cybersecurity. For online purchases, we found that the information included in the product listing should be compatible with assistive technologies for the BLV community.

58. The Commission has exercised authority in other contexts to secure both software and firmware to prevent unauthorized modification that would compromise a device or the data it transmits. For example, in adopting technical rules for the Citizens Broadband Radio Service (CBRS), the Commission required end user devices to "contain security features sufficient to protect against modification of software and firmware by any unauthorized parties" and required that such devices "be able to protect the communication data that are exchanged between these elements." The Commission adopted a further obligation for identified security vulnerabilities to be resolved on a going-forward basis, and encouraged industry to develop best practices for end-to-end security that can be validated through the certification process.97 By way of further example, in the 5 GHz band, the Commission, noting the potential for reprogramming of unlicensed national information infrastructure (U-NII) devices to operate outside of authorized device parameters, similarly adopted security measures requiring manufacturers to prevent software changes that would result in this outcome. Declining to mandate specific software security measures, the Commission required manufacturers instead to document their methods. In addition, the Commission's rules require security protocols and procedures to ensure the integrity of transmission related between and among white space devices and databases.

The white spaces and spectrum sharing databases do provide a compelling model for the FCC to run or authorize an IoT product registry in the form of a programmatic database that is accessible by third parties. Some of the cybersecurity best practices such as sending encrypted data across the in-home network and the public internet could run parallel to the rules set up for the 5GHz spectrum, although those would need to be retroactively applied to the 2.4 GHz band where most IoT devices currently operate.

Thank you very much for providing us the opportunity to provide feedback on the FCC's cybersecurity trust mark program. Consumer Reports strongly believes that, correctly implemented, this program will radically improve IoT cybersecurity practices and provide consumers with important and digestible information for them to make informed decisions when purchasing IoT devices. We look forward to working closely with the FCC and other stakeholders in making this program a success.

Respectfully submitted,

Stacey Higginbotham, Policy Fellow

Justin Brookman, Director of Tech Policy