NATIONAL ASSOCIATION OF Manufacturers

Charles Crain

Vice President,
Domestic Policy

October 6, 2023

Marlene H. Dortch
Secretary
Office of the Secretary
Federal Communications Commission
45 L Street NE
Washington, DC 20554

Re: PS Docket No. 23-239; FCC 23-65 FR ID 166265: Cybersecurity Labeling for Internet of Things

To whom it may concern:

The National Association of Manufacturers ("NAM") appreciates the opportunity to provide comment to the Federal Communications Commission ("FCC") on its notice of proposed rulemaking ("NPRM") to establish a voluntary cybersecurity labeling program for "smart" or "Internet of Things" ("IoT') devices.[1]

The NAM is the voice of the manufacturing community and the leading advocate for a policy agenda that helps manufacturers compete in the global economy and create jobs across the United States. The NAM is the largest U.S. manufacturing association, representing small and large manufacturers in every industrial sector and in all 50 states.

Many NAM members manufacture connected devices that could participate in the proposed IoT Cybersecurity Labeling Program. These modern, innovative products offer efficiency and convenience to consumers, and manufacturers are proud to be at the forefront of developing this next-generation technology. At the same time, manufacturers believe strongly in protecting consumers from cybersecurity-related risks associated with these devices. As the NPRM notes, increased connectivity—in more places within our homes and our lives—leads to increased opportunities for bad actors to access and use Americans' smart devices for their own nefarious ends.

Manufacturers of IoT devices continue to take steps to enhance the cybersecurity measures implemented within these devices in order to secure them against threats and ensure that consumers are protected to the maximum extent possible. The FCC's proposed labeling program is thus an exciting opportunity for companies to show the progress they have made in this important arena, and for the industry to cohere around a set of practical, implementable best practices to protect the American people. The promise of this program makes it all the more important that the FCC ensure that it works as well as possible for both manufacturers and consumers; the agency also should undertake a thorough consumer education effort to help consumers understand and utilize the program. To drive robust participation in the program and enhance cybersecurity protections for consumers, the NAM respectfully encourages the FCC to work closely with industry to finalize criteria and procedures that remain voluntary but, when implemented, prove workable for manufacturers and trusted by consumers.

[1] *Cybersecurity Labeling for Internet of Things*, 88 Fed. Reg. 58211 (25 August 2023). PS Docket No. 23-239; *available at* https://www.govinfo.gov/content/pkg/FR-2023-08-25/pdf/2023-18357.pdf.

I. The FCC should undertake a collaborative, iterative process of industry engagement before finalizing the proposed program.

The NAM appreciates that the FCC is seeking public comment as it works to establish a voluntary cybersecurity labeling program for IoT devices, and manufacturers view the opportunity to comment as a positive first step. However, it is critical that the FCC take the appropriate time to fully consider the details necessary for a successful cybersecurity labeling program in order to ensure that the program is both effective and workable.

Manufacturers are innovators and leaders when it comes to cybersecurity. As technology and its associated cybersecurity risks evolve, so too do manufacturers' cyber strategies. In order for the proposed cybersecurity labeling program to be effective, its requirements must reflect the breadth and depth of the industry's expertise and innovation. The FCC also must account for changes in, and potential cybersecurity risks posed by, third-party software that consumers may install and run on connected devices. A collaborative, iterative process with robust opportunity for industry engagement will ensure that the program is maximally useful for consumers—and implementable for manufacturers.

The NAM respectfully encourages the FCC to convene a series of technical industry roundtables following the close of the comment period on the NPRM. Such forums will allow manufacturers of IoT devices and industry experts to engage with policymakers, consumer protection advocates, and other stakeholders (such as retailers) in service of an effective, workable labeling program. Absent robust industry engagement, the FCC runs the risk of finalizing a program with unclear, impractical, or outdated requirements, which would increase risks to consumers and decrease industry participation. Instead, manufacturers urge the FCC to invite the industry to the table for iterative rounds of constructive feedback and deliberation.

II. The cybersecurity labeling program should remain voluntary.

Manufacturers believe strongly in the need for robust cybersecurity protections for connected devices. Nevertheless, the NAM appreciates that the FCC's proposal emphasizes that the program would be voluntary, and manufacturers respectfully encourage the agency to take steps to underscore the voluntary nature of the program as it is finalized and implemented.

First and foremost, the FCC must be clear about what a cybersecurity label means under the program: that a company has implemented and taken the steps to have verified certain cybersecurity protections. While participants in the program will undoubtedly be proud of receiving such recognition, companies choosing not to participate must not be accused or suspected of failing to adequately secure the devices they produce. A company might secure its products via measures and protections different than those recommended under the program, or it might have chosen not to undertake the cost and burdens associated with the program's verification procedures, or the product or product category in question might present a different risk profile for consumers and thus necessitate a distinct cyber strategy. In brief, while the existence of a program label should mean that a product is designed to be safe and secure pursuant to the program's guidelines, the absence of a label should not necessarily mean that a product is risky.

The NAM is concerned and disappointed that an FCC commissioner has stated that the absence of an FCC cybersecurity label should "serve as a warning: this device is not safe."[2] The NAM respectfully encourages the FCC not to adopt this reasoning when it adopts the final program—which, again, should remain voluntary. Just as it is not possible to guarantee that products in

[2] *See* Statement of Commissioner Nathan Simington re: *Cybersecurity Labeling for Internet of Things* (10 August 2023). *Available at* https://docs.fcc.gov/public/attachments/FCC-23-65A4.pdf.

compliance with the labeling program's requirements are immune from evolving cybersecurity threats, it is not the case that products not participating in the program are automatically unsafe.

Similarly, the NAM encourages the FCC to exercise restraint with respect to enforcement under the program. The NAM strongly agrees with the FCC that the cybersecurity label must be "a trusted and valuable resource to purchasers."[3] To that end, enforcement proceedings may be appropriate for companies fraudulently attempting to utilize the label. However, companies whose products cannot be updated while in use (e.g., to receive updates in accordance with evolving cybersecurity standards) or otherwise fall out of compliance with the program's requirements as technology advances should not be subject to enforcement beyond the simple removal of the label itself. The FCC should recognize the difference between knowing, intentional noncompliance and inadvertent mistakes that may have resulted from changing criteria or process-related errors.

The NAM is concerned that the NPRM raises the spectre of more draconian measures, such as "show cause orders, revocation proceedings, forfeitures, consent decrees, cease and desist orders, and penalties," or even the involvement of the Department of Justice, without accounting for this distinction.[4] Such approaches are not appropriate for errors that arise despite companies' good faith efforts to comply with a voluntary program, especially given certain devices' technical limitations—and seeking to impose them could disincentivize companies from participating in the program in the first place.

Finally, even as manufacturers urge the agency not to impose participation in the program as a *de facto* mandate, the industry understands that participation will likely be widespread in certain product categories given consumer and retailer interest. It is thus critical that the FCC follow appropriate rulemaking procedures as it takes steps to refine and finalize the voluntary program, and if it updates the program in the future. In particular, the NAM respectfully encourages the agency to conduct robust cost-benefit analysis, as required by the Administrative Procedure Act, on any processes and criteria included in the program. Similarly, any future updates to the program must undergo notice-and-comment rulemaking. Though participation in the program should not be mandatory across the industry, some companies may face pressure to seek the imprimatur of the government as to certain products' cybersecurity. As such, it is critical that the program's requirements be appropriately calibrated and that their benefits outweigh their costs. Manufacturers urge the FCC not to use the program's voluntary nature to avoid necessary and appropriate stakeholder engagement and rulemaking processes.

III. The FCC should ensure that the process by which products receive a cybersecurity label is trusted, practical, and flexible.

The NPRM contemplates designating certain third-party entities as Cybersecurity Labeling Authorization Bodies ("CyberLABs"); these CyberLABs would be charged with assessing products' compliance with the program's requirements. The NAM strongly agrees with the FCC that CyberLABs must be qualified to understand and administer the program. The NAM also believes that much of the assessment and testing necessary to evaluate compliance with the program can be done by the manufacturer of an IoT device.

CyberLAB Accreditation

Industry and the public must be able to trust the expertise of the CyberLABs so that their determinations can be relied upon across a wide range of products. To ensure this trust, CyberLABs

[3] Proposed Rule, *supra* note 1, at 58220.

[4] *Ibid.*

must possess the necessary technical credentials and act as a disinterested third party in order to provide consistent, expert analysis. The NAM respectfully encourages the FCC to institute a strong accreditation program to ensure that only the highest quality entities are able to qualify as CyberLABs. Such a program should verify that a CyberLAB has sufficient subject matter experts to evaluate products across a wide range of industries. It should also make certain that the CyberLAB has in place (and will indefinitely maintain) guardrails to protect companies' confidential information, data, and intellectual property. CyberLABs will be charged with receiving and processing important and sensitive information, so any failure to appropriately protect that information and guard against both inadvertent leaks and intentional hacks could have devastating consequences—both to participants in the program and the program itself.

Further, a critical part of the accreditation process should be ensuring that a CyberLAB has robust protections against potential conflicts of interest. The NPRM indicates that the FCC expects the CyberLABs to levy fees for processing applications under the program; this fee-for-accreditation structure will necessitate robust protections to ensure that CyberLABs focus on the underlying mission of protecting the public rather than boosting their revenues. Manufacturers urge the FCC to take steps to protect the integrity of the program against these potential conflicts.

Manufacturer Testing and Self-Assessment

The NPRM solicits comment on whether manufacturers should "be allowed to perform testing and self-assessment" of their own products, subject to third-party review.[5] The NAM strongly believes that such an approach would appropriately balance efficiency, accuracy, and consumer protection while contributing to the success of the cybersecurity labeling program; it would also allow manufacturers to better protect sensitive and confidential information about their products.

Under a self-assessment-based program, manufacturers should be permitted to assess their compliance with the program's requirements and, if applicable, run a series of tests internally to determine whether a given product meets those requirements. Self-testing would allow for accurate and reliable tests, as the manufacturer of a product knows its operations and vulnerabilities much more intimately than a third-party CyberLAB could. Additionally, self-testing would significantly decrease the costs of the program, and it would make it more likely that manufacturers' intellectual property remains protected—both of which are critical to supporting the further development of innovative products as well as the longevity of the labeling program.

Following internal testing and self-assessment, the manufacturer would submit the testing results to a CyberLAB for certification—at which point the CyberLAB would determine whether or not to grant approval for use of the cybersecurity label. This approach would strike an appropriate balance: the testing would be done by the entity that knows the product best (the manufacturer), while preserving the final certification for a disinterested third party (the CyberLAB). The NAM strongly believes that allowing for an initial self-assessment is the most cost-effective way to operate the program and that it will produce safer, more reliable labels on which consumers can rely.

Physical Labeling

After a company receives a cybersecurity label for its product, the FCC should be clear about how the company can communicate that information to consumers, including what verbiage is allowed or required, and how the label itself can or should be presented. Regulatory clarity is important to enabling manufacturers to ensure that the label is useful to consumers.

[5] *Id.* at 58216.

As the FCC sets these labeling criteria and procedures, the NAM respectfully encourages the agency not to mandate that companies place a physical label on the product itself or its packaging. Many companies may choose to present the label in this way, but a one-size-fits-all mandate to revamp product and packaging design would introduce significant costs to manufacturers participating in the program. Further, in some cases product or package labeling would not even benefit consumers, such as for large home appliances installed by third-party service providers. The costs and burdens of requiring physical labeling, especially absent an obvious consumer benefit, could disincentivize companies from participating in the program.

It can take years to finalize the look and feel of the outside of a device, and many products already face requirements with respect to what information can or should be conveyed to customers on the exterior of a product. The same is true of its packaging. Given that the FCC's cybersecurity labeling process can only be undertaken once a product is finalized and ready to test, it is simply not practical to force companies to go back and incorporate a new label on a product or its packaging in order to participate in the program. Consumers have a variety of methods by which they can access facts about a product in today's information economy (including online marketing materials, post-of-purchase displays, and manufacturer websites), so the FCC should avoid imposing an inflexible mandate requiring a physical label that would dramatically increase the costs and complexity of the labeling program.

IV. The criteria under the program should reflect the varying degrees of risk posed to consumers by different products.

The NAM has long called for scaled regulation depending on the risk posed by the technology, or technological application, in question.[6] IoT devices, and the various uses thereof, fall along a broad continuum from more to less risky from a cybersecurity perspective. The FCC's cybersecurity labeling program should reflect this reality.

Manufacturers support robust cybersecurity protections for all connected devices, but "robust" can and should be defined differently depending on the likelihood of a cybersecurity incident impacting a given product and the potential consequences of such an incident. For example, devices with a cybersecurity vulnerability that, if exploited, could put lives at risk or expose sensitive personal data may need more scrutiny or higher standards. At the other end of the spectrum, devices that are connected but not that "smart," that pose limited or no risks to safety or privacy, or that only connect to an external network under limited circumstances may need to be subject to a different set of criteria. The NAM respectfully encourages the FCC to allow for this flexibility in the design of the program's requirements and in companies' and CyberLABs' evaluations of a product's compliance therewith.

This flexibility should extend to renewals under the program. Annual renewals, as contemplated by the NPRM, are likely not necessary for products that pose limited risk or for which there have not been significant technological or security advancements. On the other hand, more frequent renewals might be necessary for products presenting higher risks or whose cybersecurity protections need to be updated in response to a confirmed high-risk vulnerability. The NAM would support renewal requirements being triggered by a specific inflection point that would necessitate a reexamination of a product's cybersecurity defenses. These inflection points would differ depending on the product and its applications in consumers' lives, but could include a critical vulnerability being discovered, new and relevant cybersecurity defenses becoming available, or significant updates to the product. Furthermore, criteria for the timing and substance of renewal, as with the criteria for the initial

[6] *See, e.g.,* NAM Comments on NTIA AI Accountability Policy (8 June 2023), *available at* https://www.nam.org/wp-content/uploads/2023/06/NAM-NTIA-AI-Comment.pdf, emphasizing that a "risk-based approach accounts for the diversity of current and future applications" of a technology.

certification decision, should be scaled based on the risk a given product poses to consumers' health, security, safety, and privacy.

V. The FCC should institute a strong safe harbor that ensures companies participating in the program benefit from robust liability protections.

As noted, manufacturers are dedicated to ensuring that their IoT devices offer robust cybersecurity protections. Cyber defenses are critical to protecting consumers' safety and privacy as more and more products become interconnected. Despite these efforts and companies' adherence to current best practices, cyber attacks still occur. Unknown and unforeseen vulnerabilities in products are found, and hackers develop new techniques to get around even the best defenses. Manufacturers strive to stay ahead of bad actors; companies are constantly innovating to make their devices safer and more secure. But no system is perfect.

While the FCC's cybersecurity label is important to signify that a company has taken the recommended steps to secure its product, the label is not a guarantee. Additionally, depending on the type of connected device, consumers may choose to install and run third-party software on the product. Assuming widespread participation in the program, it is virtually certain that, at some point, a bad actor will get past the defenses of a product that received approval to use the program label. In some cases, third-party software installed and run by the end-user may create a vulnerability ultimately exploited by a bad actor. It is critical that such a breach not be treated as a violation of the program by the manufacturer, nor be treated as grounds for legal liability—whether from the FCC or via private action.

The NAM strongly encourages the FCC to adopt a legal safe harbor that protects manufacturers who have taken good faith steps to protect the safety and security of their devices, as prescribed by the program. Manufacturers complying with the terms of the cybersecurity labeling program and conducting appropriate due diligence to stay abreast of and respond to new cybersecurity threats should not be held liable under the program if a breach nevertheless occurs. Similarly, in the event that the FCC implements an online registry of products participating in the program, delays in updating the registry that cause it to be out of sync with a product's protections or labeling also should not be treated as a violation of the program. The FCC also should limit liability and enhance consistency by providing for preemption of state-level laws and requirements for products participating in the program, and clarifying that the program's legal safe harbor protects companies from potential liability associated with current or future state requirements.

The lack of such a safe harbor would disincentivize participation in the labeling program. While enforcement for willful violations or intentional misrepresentations would be appropriate, it is not in manufacturers' or consumers' best interests for the FCC to unreasonably punish companies for voluntarily participating in the program and taking good faith steps to comply with its requirements when it is well known that no cyber defense can be 100% effective to thwart all attacks. As such, a robust legal safe harbor is critical to the program's success.

VI. The FCC should educate consumers about the program and encourage them to utilize cybersecurity best practices.

The FCC can also promote legal certainty and bolster the labeling program by taking proactive steps to educate consumers on what a label does and does not mean. The FCC should be clear that the label indicates that a given product has been verified to implement certain best practices and protections, which will be maintained for a specified duration, against certain threats—and that certain steps have been taken by a reliable third-party to verify said protections. The FCC should be similarly clear that the label is not an ironclad guarantee against any and all future attacks, because no such guarantees are possible.

As such, the FCC also should provide education and resources as to how consumers can help protect themselves. Many cybersecurity protections can *only* be taken by the consumer—for example, installing a software update, changing a password, or obtaining third-party software only from reliable sources—so it is vital that consumers understand that they are a critical partner in the cybersecurity effort. The FCC has an important role to play in working with manufacturers to inform consumers about cybersecurity threats and best practices, and these education efforts are vital to the success of the cybersecurity labeling program.

* * * *

The NAM commends the FCC for seeking to establish a program by which manufacturers' leading, innovative work to ensure safe and secure devices can be recognized. To drive industry participation and consumer trust in the program, it is critical that participation remain voluntary—and, for companies that choose to participate, that the program be developed with industry input, that its requirements and processes be practical and flexible, and that participants benefit from robust liability protections. Finally, consumer education about cybersecurity threats and best practices is vital to the program's success. Manufacturers look forward to working with the FCC to implement a labeling program that is workable for industry and effective for consumers.

Sincerely,

Charles Crain
Vice President, Domestic Policy