Mike Fagan
Computer Scientist
National Institute of Standards and Technology
100 Bureau Dr.
Gaithersburg, MD 20899

Re: Comments on the Revision Draft of NIST 8259 Foundational Cybersecurity Activities for IoT Product Manufacturers

Consumer Reports appreciates the chance to comment on the cybersecurity requirements for Iot Product manufacturers, and for the chance to present in December 2024 on post-market surveillance activities related to the current 8259 recommendations. We are especially pleased to see NIST prioritize cybersecurity needs throughout the connected product lifecycle by adding "Activity 5: Support Product Cybersecurity through End of Life" to the list.

The need for security in a connected device doesn't stop once the product is sold, so adding questions about how security is maintained over the entire life of the product to the framework is important. This will require customers, manufacturers and others responsible for securing a connected device to think about vulnerability disclosure programs, how to communicate the end of support periods, and more.

With that in mind we wanted to call out a few potential tweaks to the document that can reinforce the decision to consider security throughout the life (and eventual disconnection) of a connected product. We have included these below. We follow with a general discussion of points raised in the document.

"Therefore, a securable IoT product has product cybersecurity capabilities (i.e., hardware and software) and other support provided by the manufacturer or other supporting entity that customers may need to mitigate common and expected cybersecurity risks related to the use of the IoT product and its connection to customers' systems." (Section 1.1)[1]

[1] Fagan M, Megas K, Cuthill B, Marron J, Hoehn B (2025) Foundational Cybersecurity Activities for IoT Product Manufacturers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8259r1 ipd. https://doi.org/10.6028/NIST.IR.8259r1.ipd

We appreciate that this definition focuses on the myriad components that comprise a connected product and assigns a role to manufacturers that requires that they think about how customers might use the connected product and their respective risk models, but we would also like to to see the phrase "over the expected life of the product" added to this definition. Security in a connected device is an ongoing obligation and a manufacturer and product owner have to develop a framework for managing security over time as the threats evolve and the IoT product components degrade.

"Determining which components are part of an IoT product and which are not should be driven by whether removal of or disconnection from the component would break IoT product functionality." (Section 2.2)[2]

This requirement is not as clear as it could be because "product functionality" is a slippery concept. One could conceivably argue that a connected thermostat that can be manually operated from the device and still control an HVAC system absent a cloud connected or application software retains product functionality. We believe that thinking about the product in terms of advertised features as opposed to its functionality may provide a more clearly delineated standard.

Also in line with the expected lifecycle of a connected product, where a manufacturer might stop providing software support, cloud back-ends, and security updates, this document should make recommendations about how to safely decommission a product that has been connected to the internet. For example, if a piece of connected equipment stops receiving support, but still has a Wi-Fi module, are there mechanisms in place to ensure that the module is not broadcasting a soft AP, or a Bluetooth device is not continuously seeking a connection that may become a potential vulnerability? This problem is already acknowledged as part of footnote 2 in the document.

Section 2.3 lays out different entities involved in the IoT ecosystem. We think the document should add one more — bystanders. These are the entities who come into contact with the IoT ecosystem through their employment, their residence in a connected home, or other day-to-day activity. I understand that privacy is not a stated concern of this NIST IR, but bystanders can still have access to IoT ecosystems through their physical proximity. For example, consider the ability of industrial employees to pick up a random USB stick and plug it into connected equipment, potentially introducing malware. Additionally, in a surveillance state, employees or customers of a business that uses connected devices, may face security and privacy risks from being monitored and their actions saved in a connected ecosystem.

The questions asked for assessing risk management in Section 3.1 have grown in sophistication, which is appreciated. The addition of understanding the type of digital environment, what is

[2] *ibid*

required for the product to function, and the types of data created by the product are excellent. Based on our request that NIST consider the distinction between a product's functionality and its advertised features we would like to see Question 6 adjusted to ask what IoT components are required for the product to meet its advertised features. Question 9 specifically calling out the need to consider the types of data created by the product will help companies meet the demands of the U.S. Cyber Trust Mark program as well as a recently implemented Connecticut law. [3]

During the discussion of risks in Section 3.2 we suggest looking at the threat models proposed for the U.S. Cyber Trust Mark program in Appendix A of the cover letter UL provides with its technical recommendations.[4] They include, harm to individuals, harm to the device, command and control attacks, data mining, and compromising the manufacturer. The five-ponged model is more specific and covers the potential harms in a clear way. It also might be useful to create some harmonization between programs. And while the UL is making recommendations for a consumer program, the threat models are applicable across industry, enterprise and consumer settings.

We find the assessment questions included in this section excellent, and a good example of how NIST's thinking about IoT cybersecurity has evolved to meet the threats that have developed in the last five years. In Section 3.3 the recognition that there will be both technical and non-technical means to address cybersecurity goals is a welcome call out to the importance of process and business practice in supporting security. Tying to customer expectations of product security to the robustness of the mechanisms in place to support it is also a welcome change. NIST is trying to straddle the line between creating a framework that addresses the broad nature of IoT products in a way that is flexible and recognizes that different products have different use cases.

In the list of questions addressing the non-technical means of securing a device we'd like to see NIST address access that manufacturer or device installers and maintainers might have to the data thrown off by the IoT product. We have seen cases where manufacturer employees or installers have access to IoT data and/or systems and then access camera or location data to stalk or monitor the customers of the system without their knowledge. Requiring manufacturers to protect access to data to a limited pool of authorized users, and setting up a notification when those users make changes would be a good additional practice in this section.

In Section 4.1 NIST asks "which product cybersecurity capabilities enable post-market cybersecurity support?" and then mentions software updates. We'd like to see a deeper discussion on this element because product design specifications such as sufficient memory, the

[3] An Act Concerning Consumer Protection and Safety. CT. Public Act No. 25-44. Senate Bill 3 (2024-2025) Sec. 2

[4] US Cyber Trust Mark, Technical Requirement Recommendation. Filed June 16, 2025. FCC Docket No. 23-239 https://www.fcc.gov/ecfs/document/10616194651304/1

expected support life of a chip's firmware, and how flexible the underlying hardware or software design decisions support new cryptography all have a role to play in how long a connected device can continue to achieve software updates and remain secure.

Ultimately, we find this framework is continuing to mature with the IoT product industry and the experiences companies and customers have had in the last five years of building, owning and maintaining these devices. We appreciate the work that NIST has put into the original framework and its evolution. Thank you for considering our comments. If you have any questions, please reach out to me at stacey.higginbotham.consultant@consumer.org.

Sincerely,

Stacey Higginbotham
Policy Fellow
Consumer Reports