hackerone

July 14, 2025

VIA EMAIL: iotsecurity@nist.gov

National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Re: Request for Information on NIST’s Foundational Cybersecurity Activities for IoT Device Manufacturers

Dear Sir or Madam:

HackerOne Inc. (HackerOne) submits the following comments in response to the National Institute for Standards and Technology (NIST)’s draft revision of NIST IR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers.[1] We appreciate the opportunity to provide input, and we thank NIST for its continued leadership in driving public and private solutions towards a more secure and resilient Internet of Things (IoT) ecosystem.

By way of background, HackerOne is a global leader in offensive security solutions. Our HackerOne Platform combines AI with the ingenuity of the largest community of security researchers to find and fix security, privacy, and AI vulnerabilities across the software development lifecycle. The platform offers bug bounty, vulnerability disclosure, pentesting, AI red teaming, and code security. We are trusted by industry leaders like Amazon, Anthropic, Crypto.com, General Motors, GitHub, Goldman Sachs, Uber, and the U.S. Department of Defense.

Invested in improving the security of connected devices, HackerOne strongly supports NIST’s efforts to refine the foundational activities outlined in IR 8259. Specifically, we recommend that NIST offer clear expectations alongside baseline recommendations. Providing more definitive answers on best practices would help ensure greater consistency across the industry and give manufacturers a stronger foundation on which to build their cybersecurity programs.

1. Vulnerability Reporting and Disclosure

HackerOne appreciates NIST’s inclusion of vulnerability reporting and disclosure capabilities in the revised draft, and the recognition that while primarily procedural, these capabilities are critical to support product cybersecurity. We strongly agree with NIST’s assertion that vulnerability response programs, vulnerability database monitoring, and the use of threat intelligence services are key components of post-market cybersecurity management. These

[1] NIST IR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers, https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8259r1.ipd.pdf

activities provide vital pathways for identifying and remediating vulnerabilities in a timely manner, especially in rapidly evolving threat landscapes.

The draft also rightly acknowledges that cybersecurity mitigations such as software updates are not just product improvements—they are essential risk reduction tools that customers rely on to maintain the security of their devices and the systems they connect to. However, these post-market mitigations cannot occur unless vulnerabilities are first discovered and reported. For that reason, a manufacturer's ability to intake, assess, and respond to vulnerability reports—both during and after the product's supported lifecycle—is fundamental to a secure IoT ecosystem. We recommend NIST go further and explicitly recognize Vulnerability Disclosure Policies (VDPs) as a foundational expectation for all IoT device manufacturers. VDPs offer a structured and effective framework for receiving, identifying, and triaging vulnerability reports. Often referred to as the internet's "see something, say something" policy, VDPs encourage individuals to report security risks they encounter, allowing organizations to address these issues promptly before they can be exploited.[2] This proactive approach helps prevent data breaches, minimize security threats, and reduce the overall impact of vulnerabilities. The value of a VDP extends across the full lifecycle of a device. During development and pre-release testing, early disclosure mechanisms allow organizations to identify and fix vulnerabilities before they are shipped. After a product is released, the variety of real-world environments and configurations can surface issues not evident during internal testing.

In addition, HackerOne believes it is equally important to recognize other effective methods of identifying vulnerabilities, such as Bug Bounty Programs (BBPs), which complement VDPs by incentivizing independent researchers to uncover and responsibly disclose security flaws. In comparison to VDPs, BBPs also allow organizations to seek security information on specific systems, which they can specify in a program policy.

To support consistent and effective implementation, HackerOne recommends that NIST include more specific guidance on the structure and scope of both VDPs and BBPs in the revised IR 8259. At a minimum, NIST should encourage manufacturers to clearly define which systems are in scope and outline permissible testing methods for BBPs. For VDPs, manufacturers should establish accessible reporting channels and commit to timely acknowledgment, remediation transparency, and public communication. These elements together foster a more collaborative and resilient approach to vulnerability management.

Overall, HackerOne supports NIST's leadership in elevating the importance of vulnerability reporting and disclosure and encourages further specificity in the revised IR 8259. We believe that detailed, publicly accessible, and well-resourced VDPs—and, where appropriate, BBPs—should be baseline expectations for IoT manufacturers.

2. Support for Independent AI Testing

[2] HackerOne VDP Report, https://www.hackerone.com/sites/default/files/2021-03/vulnerability-disclosure-policy-what-is-it-why-you-need-one-how-to-get-started.pdf

HackerOne encourages NIST to recognize the emerging role of artificial intelligence (AI) in IoT device functionality and the corresponding need for independent AI testing as a critical cybersecurity activity. Although AI security is not explicitly addressed in the current draft of IR 8259, its growing integration into connected devices introduces novel attack surfaces and operational risks that traditional security testing methods are not always equipped to identify or mitigate.

Manufacturers can and should rely on AI red teaming to uncover how adversaries might exploit vulnerabilities in AI-enabled systems—whether they involve typical cybersecurity flaws or non-security vulnerabilities. Independent AI testing plays a vital role in both the pre-deployment and post-deployment phases of the product lifecycle.

For IoT manufacturers, integrating independent AI testing is essential to proactively identify and address unique risks posed by AI components before devices reach consumers. Pre-deployment AI red teaming allows manufacturers to discover hidden vulnerabilities that could lead to exploitation, unsafe device behavior, or failure of the device to operate as intended. After deployment, ongoing AI testing is equally important, as real-world use can expose new issues or attacks that affect AI performance and security.

By embracing independent AI testing, IoT manufacturers can improve the security, reliability, and performance of their AI-enabled devices, enabling them to better protect end users and infrastructure. HackerOne recommends that NIST explicitly include independent AI testing in its guidance as a foundational element of secure IoT device development and maintenance.

* * *

HackerOne appreciates NIST's ongoing leadership in advancing IoT cybersecurity and encouraging manufacturers to prioritize security throughout the product lifecycle. We recognize the value of the foundational activities outlined in this publication but would support NIST taking a larger role in guiding manufacturers to better understand and meet their customers' cybersecurity needs. We look forward to continued collaboration and stand ready to support NIST's efforts.

Respectfully Submitted,

Ilona Cohen
Chief Legal and Policy Officer
HackerOne