Comments to Request for Information on NIST's Foundational Cybersecurity Activities for IoT Device Manufacturers

July 14, 2025

The Hacking Policy Council ("HPC") submits the following comments in response to the Request for Information (RFI) related to National Institute of Standards and Technology (NIST)'s draft revision of NIST IR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers.[1] We thank NIST for its continued leadership in shaping a more secure and trustworthy cybersecurity environment for emerging technologies, including the Internet of Things (IoT).

The HPC is a group of experts dedicated to creating a more favorable legal, policy, and business environment for good faith security research, penetration testing, independent repair for security, and vulnerability disclosure and management.[2] From this perspective, we broadly support the approach NIST has taken in updating IR 8259 and commend the inclusion of post-market cybersecurity considerations and guidance for manufacturers. We respectfully offer the following recommendations, which we believe would further strengthen the document and ensure comprehensive coverage across the pre-market, post-market, and end-of-life phases of the device lifecycle.

1. Support for Vulnerability Disclosure Policies (VDPs)

The HPC commends NIST for raising key questions in the draft regarding how customers can report suspected security issues, whether such reports will be accepted after the end of support, and how manufacturers might respond to reports during and after the end-of-life phase. These questions rightly acknowledge that the cybersecurity responsibilities of IoT manufacturers do not end at the point of sale. They also signal an important recognition that clear, persistent reporting mechanisms are essential for effective vulnerability management over time.

Building on this important inclusion, we recommend that NIST go further by explicitly identifying Vulnerability Disclosure Policies (VDPs) as a foundational and necessary element of any secure IoT product development strategy. While it is useful to frame vulnerability reporting as a process manufacturers should consider, the reality of today's evolving threat landscape demands a more direct expectation. Without formal VDPs, manufacturers risk missing critical vulnerabilities that could have otherwise been identified and remediated.

---

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

[2] Hacking Policy Council, https://hackingpolicycouncil.org.

Establishing a VDP before a product reaches the market enables researchers, testers, and other trusted stakeholders to report vulnerabilities discovered during development and internal testing. Early engagement of this kind can help prevent critical vulnerabilities from reaching end users, reduce the likelihood of zero-day exploits, and demonstrate the manufacturer's commitment to security-by-design.

After deployment, a product enters increasingly diverse and unpredictable operating environments, which often reveal new vulnerabilities that were not evident during development or testing. Maintaining an open and active VDP during the post-market phase allows manufacturers to stay informed about these emergent risks and act on them rapidly and efficiently. Importantly, even after a device reaches its end-of-life phase, its potential to impact users and connected systems persists. Many IoT devices, particularly those in industrial or embedded applications, remain in use for years beyond the point at which official support ends. In these cases, manufacturers should still accept and assess vulnerability reports and, where feasible, provide mitigation guidance or security advisories. While it may not always be possible to issue patches, acknowledging and responding to reports can significantly reduce risk for legacy users and the broader ecosystem that relies on interconnected systems.

We urge NIST to include an explicit recommendation that all manufacturers publish and maintain a VDP, including a clear point of contact, a response process, and timelines for responding to reports. To support a consistent and scalable approach, we encourage NIST to reference internationally recognized frameworks, such as ISO/IEC 29147[3] and ISO/IEC 30111. These standards offer a tested and proven foundation for implementing and managing VDPs and will help align practices across manufacturers and industries.

2. Incentivizing Bug Bounty Programs (BBPs)

In addition to maintaining a VDP, manufacturers should be encouraged to consider implementing bug bounty programs (BBPs). BBPs offer structured opportunities for independent researchers to find and responsibly report vulnerabilities in exchange for financial incentives.

BBPs complement and reinforce the goals outlined in the questions listed on page 26 of the draft, particularly regarding how manufacturers accept and respond to vulnerability reports, verify third-party software security, and minimize risks in deployed products. These questions are an excellent foundation for evaluating the maturity of an organization's software security posture. HPC recommends that NIST go a step further by explicitly encouraging BBPs as a best practice—particularly for manufacturers producing widely deployed, high-impact, or critical infrastructure IoT products. Threat actors continually probe manufacturers' products, looking to find and exploit vulnerabilities. By leveraging BBPs to safely surface and fix vulnerabilities before the threat actors find and exploit them, manufacturers can avoid the significant financial and reputational harm of a data breach. While not all manufacturers may have the capacity to

[3] ISO/IEC 29147:2018, Information technology – Security techniques – Vulnerability disclosure, International Standards Organization, Oct. 2018, https://www.iso.org/standard/72311.html. ISO/IEC 30111:2019, Information technology – Security techniques – Vulnerability handling processes, International Standards Organization, Oct. 2019, https://www.iso.org/standard/69725.html.

operate a full-scale program, many third-party platforms offer customizable options for organizations of various sizes and resource levels.

3. Adopt AI Red Teaming

As artificial intelligence and machine learning become increasingly integrated into IoT devices, these technologies introduce a unique set of risks that traditional software security methods are not fully equipped to address. These could include adversarial inputs designed to trick models, data poisoning that manipulates training datasets, and unintended outputs. Given the unique nature of these threats, NIST should explicitly recommend AI red teaming as a key component of modern IoT security testing, spanning both the development and post-deployment phases.

AI systems should be rigorously tested not only for traditional security vulnerabilities but also for non-security flaws. During the development phase, testing helps identify and mitigate risks early, while also ensuring that trustworthiness considerations are built into the design. AI red teaming during this stage is especially valuable because it allows developers to simulate adversarial scenarios and stress-test how a system behaves under manipulated inputs. As with traditional security practices, testing is also appropriate when the AI system is deployed in context, as well as following any significant system changes. Given the evolving nature of AI model training data, attack techniques, mitigations, and features in both security and trustworthiness, it's important to continue testing post-deployment to address emerging threats and continually enhance the system's resilience.[4]

* * *

HPC supports NIST's leadership in developing cybersecurity guidance that reflects the complexity of modern IoT ecosystems. We believe that the inclusion of explicit requirements and recommendations around VDPs, BBPs and AI red teaming will strengthen NIST IR 8259 and better prepare manufacturers for the realities of securing IoT devices over time.

We thank NIST for the opportunity to provide these comments and welcome continued engagement on this issue.

Sincerely,

Hacking Policy Council

---

[4] HPC Comments to Request for Information Related to NIST's Assignments Under the Executive Order Concerning Artificial Intelligence, https://cdn.prod.website-files.com/660ab0cd271a25abeb800460/660ab0cd271a25abeb8005c5_Hacking%20Policy%20Council%20-%20comments%20to%20NIST%20re%20AI%20red%20teaming%20-%20240202.pdf.