
Sharpening the Focus on Product Requirements and Cybersecurity Risks:

Data: 2025-09-30 14:07:28

Autor: Inteligência Against Invaders

Over the past few months, NIST has been revising and updating [Foundational Activities for IoT Product Manufacturers \(NIST IR 8259 Revision 1 Initial Public Draft\)](#), which describes recommended pre-market and post-market activities for manufacturers to develop products that meet their customers' cybersecurity needs and expectations. Thank you so much for the thoughtful comments and feedback throughout this process; 400+ participants across industry, consumer organizations, academia, federal agencies, and researchers shared feedback in both the [December 2024](#) and [March 2025](#) workshops—as well as through written comments on the initial public draft. Others came to the virtual [Discussion Forum Event](#) in June to discuss updates, share initial ideas for a worked example of NIST IR 8259, and explore [topics from an essay](#) on planned updates to [NIST SP 800-213/213A](#).

NIST shared two workshop summary reports ([December 2024 Workshop](#) and [March 2025 Workshop](#)) and distilled the comprehensive changes that expand the focus on IoT products, highlighting product cybersecurity capabilities as central to IoT cybersecurity.

What Happens Next?

Serving as a culmination of this collaborative effort, we are announcing the release of our latest resource, [NIST IR 8259 Revision 1 Second Public Draft](#), today.

For the second draft, we've focused on incorporating feedback from the community to ensure the resource remains relevant and practical. Here's a look at what's been updated:

- **Splitting and Revising Activities:** NIST looked at splitting certain activities (e.g., Activity 3 became Activities 3 and 4) and adding a new one (i.e., Activity 0) to better reflect feedback and clarify the process steps in 8259. Focus was given to whether revised activities captured and focused attention on the intended requirements and addressed the comments received.
- **Focus on Risk Assessment and Threat Modeling:** There was a review of how risk assessment and threat modeling are incorporated into the document, ensuring that the activities and examples reflect a robust approach to identifying and mitigating risks. This includes the need for initial risk assessments and the importance of integrating threat information into the process of determining appropriate cybersecurity capabilities for the product.

-
- **Inclusion of Standards and References:** NIST has considered how to incorporate useful references—for example, the use of the NIST Cybersecurity Framework into the newly added Activity 0—and where new examples could illustrate application across different industries.
 - **Document Structure and Clarity:** Comments about the overall structure, clarity, and organization of the document were reviewed. NIST considered how to present information in a way that is accessible and actionable for different audiences. Section 2.6 was added to clarify the relationships between customer needs and goals, means, and product cybersecurity capabilities. Paragraphs were added to 1.1 *Purpose and Scope*, 2.1 *Product Cybersecurity and System Cybersecurity*, and 2.3 *Entities in an IoT Product Ecosystem*.

As discussed at the June discussion forum, we have also been reviewing sample use cases for a worked example of NISTIR 8259 Revision 1 and will have an update to share with the community later in the fall. The worked example demonstrates the process of a manufacturer sequentially progressing through the activities while developing a representative IoT product. Balancing the need for specificity in examples with the requirement to keep the document broadly applicable across sectors, NIST has considered different approaches to presenting the worked example.

We are committed to advancing IoT cybersecurity and fostering a secure ecosystem for connected product technologies across industries. We look forward to hearing your feedback on the second public draft of NIST IR 8259 during our public comment period, which closes on October 31, 2025. We plan to engage in additional conversations with the community, particularly during our workshop on December 16-17, 2025, and provide updates as we work to finalize NIST IR 8259 Revision 1.