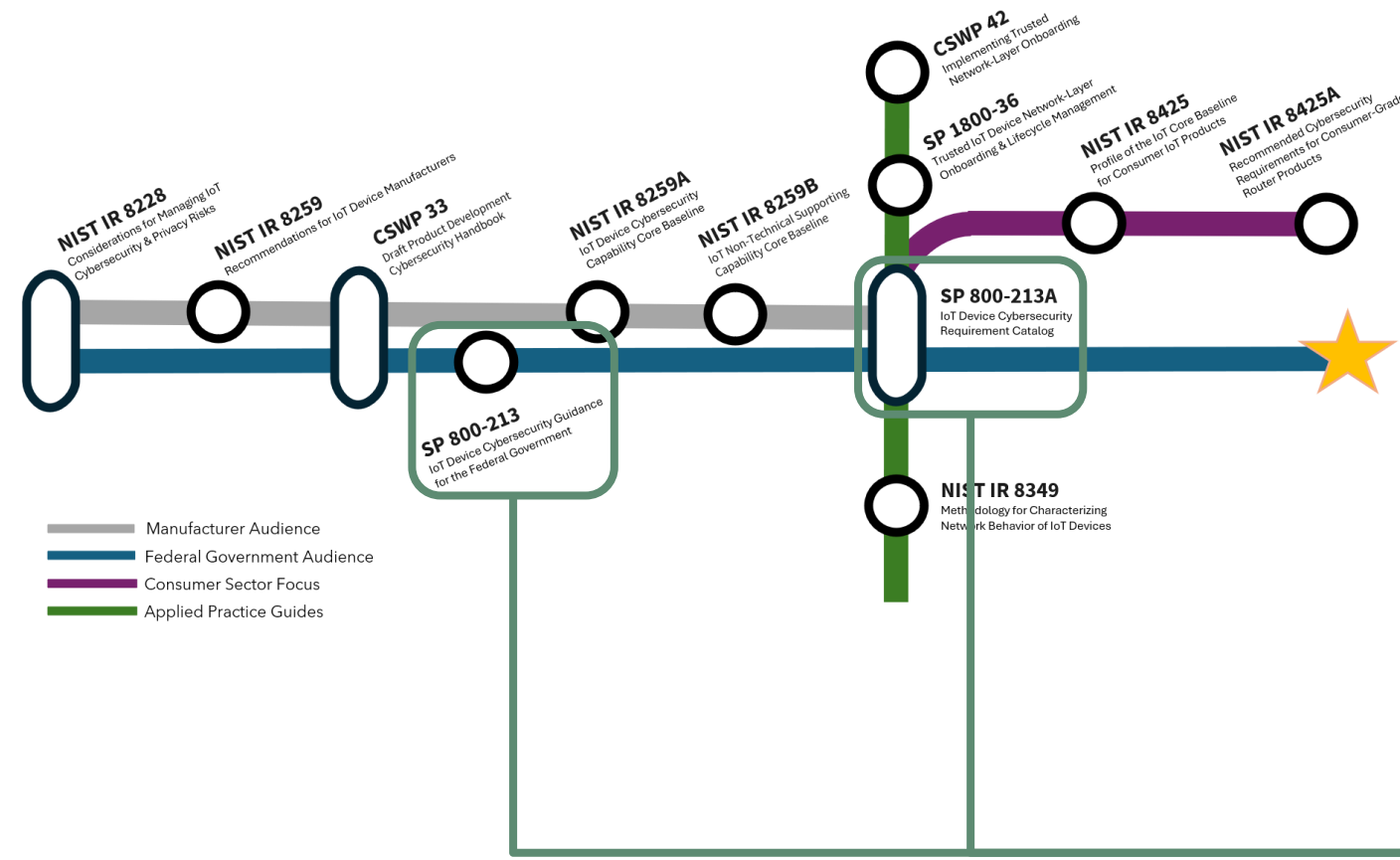




Cybersecurity for IoT Program Update

Michael Fagan, NIST
September 1st, 2026

NIST Cybersecurity Program for IoT



- NIST Cybersecurity for Internet of Things (IoT) Program was established in 2017 in response to EO 13800 (Strengthening the Cybersecurity of Federal Networks & CI).
- Since then, the Program has:
 - Published 20+ documents (with 500k+ downloads)
 - Held 12+ public workshops
 - Engaged with 3,500+ stakeholders
 - Processed 2,200+ comments
- The Program is focused on creating **usable resources** for cyber professionals seeking an **enterprise approach to managing risk for connected devices** deployed throughout their organizations.
 - Response to challenges from emerging tech, including:
 - AI-enabled cyber attacks
 - Deployment of AI in IoT
 - Quantum-resistant crypto

The Program is updating our current security guidelines and looking to how we can provide more comprehensive, usable resources for managing connected product security.

Updating existing guidelines



Draft SP 800-213 rev1 IPD

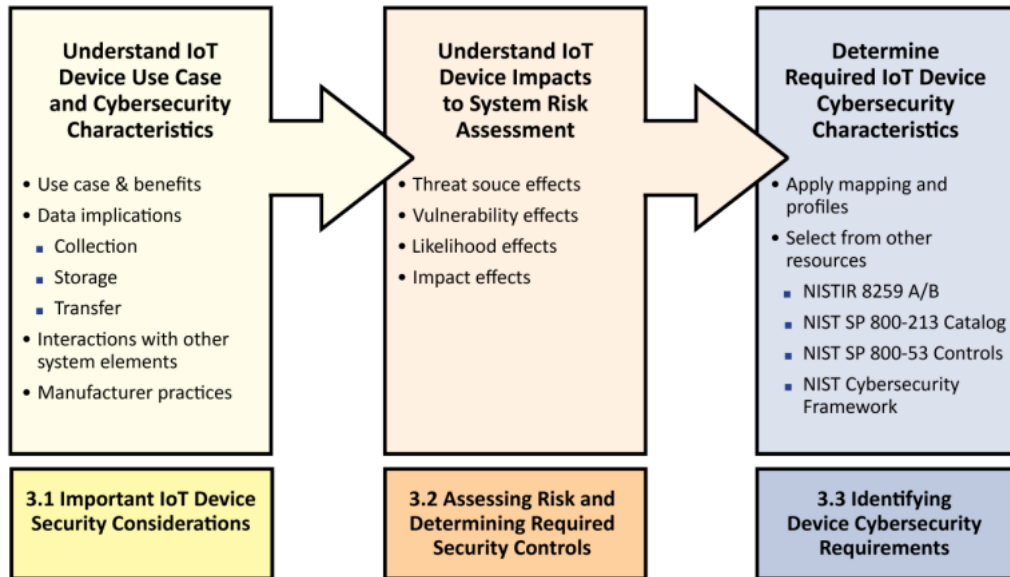
- We've published the [draft IPD](#), with the comment period closing Aug 24, 2026.
- IPD reflects current needs, with lessons learned from stakeholders.
- Focused on providing clearer guidance, more relevant content, and better alignment to today's environment.
- Notably, we shift towards speaking about “products”—better capturing how these connected devices function and are deployed. The draft remains focused on integrating products that were not previously part of the system (“new products”).

Updating SP 800-213A

- Team is preparing to begin revision of [SP 800-213A, IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog](#).
- Pre-Draft Call for Comments posted August 31, 2026.
<https://csrc.nist.gov/pubs/sp/800/213/a/r1/iprd>
- Goal is to hear from stakeholders on how to make this more usable / applicable for today's landscape, including with increased deployment of emerging technologies (e.g., AI, post-quantum readiness).

SP 800-213 Update – Initial Feedback

SP 800-213 provides a frame of reference and process to guide the identification of *IoT product cybersecurity requirements* for IoT products that are to be connected to federal systems.



Support for shift to IoT “products”, quality of life updates, and other changes made for the initial public draft.

Suggestions for improvements and features that can enhance readability.

Calls for further discussion of cybersecurity governance challenges and solutions, as well as ensuring alignment with other guidelines.

SP 800-213A Call for Comments



Given the shift from “devices” to “products,” how should we align NIST SP 800-213A with NIST SP 800-213 Rev. 1 in relation to IoT products?

Addressing IoT Products

How is your organization using IoT? Are there novel IoT use cases we should consider in the update?

Novel and Unique IoT Adoption and Use Cases

How can NIST SP 800-213A appropriately handle situations in which an organization combines multiple off-the-shelf components to create an IoT sub-system akin to an IoT product?

Addressing Unique and Tailored IoT Deployments

The content in NIST SP 800-213A was sourced primarily from NIST SP 800-53 Rev. 5 & the NIST Cybersecurity Framework (CSF). What other sources should we look to?

Foundational Guidelines to Base our Work Upon

Document Usability

How can descriptions and discussions for each capability in NIST SP 800-213A best help practitioners identify appropriate IoT product cybersecurity capabilities in different operational environments?

These questions were officially posted to CSRC as a Pre-Draft Call for Comments for SP 800-213A:

<https://csrc.nist.gov/pubs/sp/800/213/a/r1/iprd>

Additional Program Updates



The Program looks to provide comprehensive, usable resources for managing connected product security.

IoT & OT Cybersecurity

- Exploring overlaps in IoT and OT cybersecurity concerns in response to increasing connectivity, and the need to establish effective cybersecurity controls for a heterogenous and dynamic landscape.
- Strengthening partnership with NIST's OT cyber program.

Adapting to Risk in Context

- Planning deliverables (e.g., model, handbook, tool) to help risk managers and CISOs manage IoT security based on organizational context.
- This will move beyond establishing or expanding an “academic exercise,” synthesizing existing resources (from NIST and other authorities) and applying them in a way that supports real decisions, prioritization, and risk management.

Tracking US Cyber Trust Mark

- Executive Order 14306 directs update of Federal Acquisition Regulations to “require vendors to the Federal Government of consumer Internet-of-Things products, as defined by 47 CFR 8.203(b), to carry **United States Cyber Trust Mark** labeling for those products.”
- NIST IR 8425 is the cybersecurity foundation for the US Cyber Trust Mark.

THANK YOU

CONTACT US



iotsecurity@nist.gov



@NISTcyber



NIST Cybersecurity for IoT
Program Home Page