Essay: *Planning for Updating* ***IoT Cybersecurity Guidance for the Federal Government (NIST SP 800-213 and NIST SP 800-213A)***

Introduction

Federal agencies across the government are actively deploying Internet of Things (IoT) technologies to enhance connectivity, security, environmental monitoring, transportation, healthcare, and industrial automation. Government facilities are integrating IoT-enabled security systems, including AI-powered cameras, sensor networks, automated alerts, to improve safety, disaster preparedness, and energy efficiency, while IoT solutions are enhancing data center monitoring, helping track power stability, humidity levels, and flooding risks. Specific agencies are also deploying scores of environmental IoT sensors to monitor air and water quality, generating critical data for scientific research, conservation and potentially regulatory policies, while other agencies are developing earthquake early warning systems using real-time telemetry sensors to detect seismic activity, process alerts, and distribute public notifications.

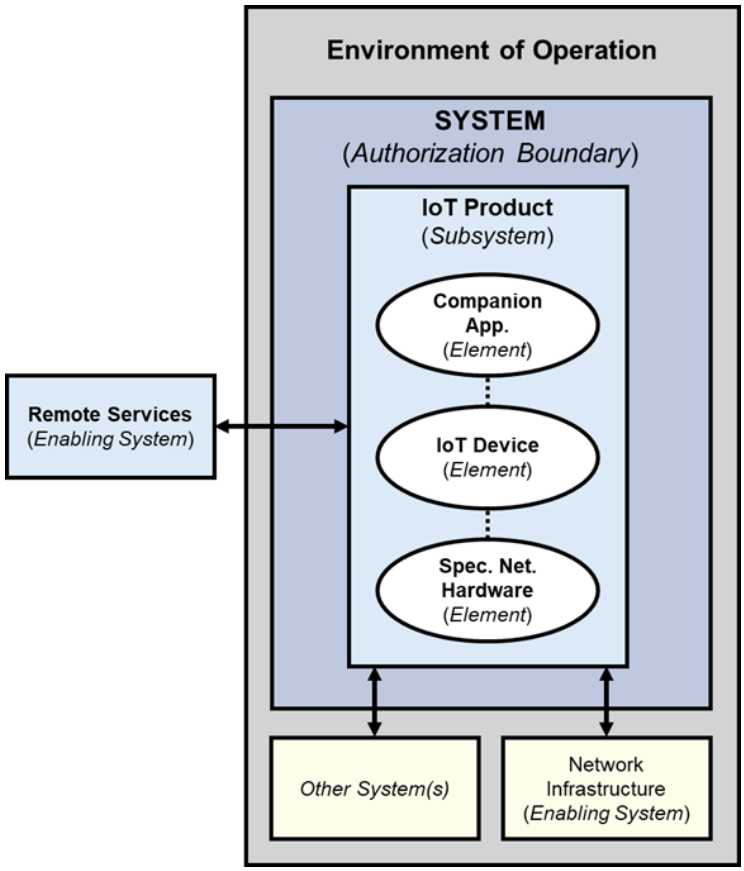
With these and other exciting IoT use cases in mind as well as requirements from the 2020 Cybersecurity Improvement Act to revise as appropriate IoT cybersecurity guidelines for the federal government at least every five years, NIST is revisiting *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*, SP 800-213, which was published in November of 2021. With the expectation to revisit and, if necessary, revise this work every five years, the Cybersecurity for IoT team is considering areas of potential revision for SP 800-213. This essay presents some example areas of revision for the community to consider while NIST engages and gathers feedback on parts of the document that could be updated. As always, NIST welcomes feedback and discussion from the community!

Example Areas of Revision

As we look for potential revisions, it helps to consider recent trends in NIST's IoT cybersecurity work and in federal agency cybersecurity.

IoT Products

When NIST SP 800-213 was written, the primary focus of NIST's IoT cybersecurity efforts was IoT devices; but since then, the aperture has expanded to consider IoT products which will always include at least one IoT device, but potentially other IoT product components as well. NIST's definition of an IoT product is meant to help scope the boundary of the product by limiting what is considered an IoT product component as those software or hardware equipment needed to meaningfully use the IoT device, particularly its "smart" features. Some IoT products will be nothing more than an IoT device, but many times devices rely on remote backends, companion applications, or specialty networking hardware (e.g., sensor base station or short-range protocol hub) to operate beyond basic features, if at all. To illustrate, the following figure shows a view of an IoT product comprised of multiple IoT product components beyond the IoT device.



SP 800-213's guidelines acknowledged that IoT devices may rely on other components to operate, but this determination was mostly left to customer organizations as the SP 800-213 guidelines focused on risk determinations with respect to the IoT device and its suite of functionality. Organizations continue to face challenges efficiently managing the risks related to the use of a wide range of IoT products with varying architectures.

NIST plans to examine how SP 800-213 can be revised to better address the adoption of IoT *products* by organizations, including considering complex network topologies and product architectures that can cross authorization boundaries. Initial discussions have revealed a few key considerations to help understand the relationship of an IoT product to the organization and the system in which it will be incorporated. One key consideration is the organization's level of integration expected for the IoT product. We can broadly consider two "levels of integration:"

1. The IoT product and local components of the IoT product are treated as part of the organization's system.
2. The IoT product is treated as a separate system from the organization's other systems.

Other considerations will exist as well, for example:

- Will the IoT product be part of a new system or part of an otherwise existing system?
- How well do the IoT product's features align to the system assumptions and objectives?

Much of the IoT device cybersecurity risk assessment guidelines described in SP 800-213's Section 3 speak to these considerations and will likely remain the same for how federal agencies consider IoT products' potential risk assessment impacts. These considerations may be generalized or expanded so that they speak to not only IoT devices, but other IoT product components as well.

Questions to consider

1. How should NIST consider IoT devices that rely on other components to operate?
2. How can SP 800-213's risk consideration guidelines for IoT be revised to address the complexities of IoT products with diverse, multi-component architectures?
3. Could NIST develop additional catalogs beyond the *IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog*, SP 800-213A's device cybersecurity capabilities that describe technical capabilities for other IoT product components? Would such catalogs be useful to the community?
4. In general, what guidelines would be most helpful for IoT product components such as software and remote services?

Increasing Convergence between Operational Technology (OT) and Information Technology (IT) via IoT

Internet connectivity is becoming more common in equipment that previously lacked it. Operational technology (OT) encompasses a broad range of programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment) in complex ways. Often OT systems and devices have long service lives, may be deployed in hard-to-reach locations (e.g., embedded in walls of buildings), and perform functions that were previously stand alone or only available on local networks. Examples of OT include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems.

For organizations, merging IT and OT functionality introduces the possibility of new features and functions. IoT products or systems can offer the same or similar OT functionality with additional informational technology (IT) and IoT functions. IT functions include those related to the storage and transmission of data. These functions, specifically the connectivity afforded by linking to the internet, enable IoT functions to be added to OT systems such as remote management of equipment and more precise control via continuous monitoring. Connectivity can also introduce challenges for organizations in applying cybersecurity controls to OT and some IoT products due to factors such as:

- OT equipment may use networking technologies (e.g., ethernet, Wi-Fi), but are not intended to connect to the internet.
- OT or IoT equipment may balance aspects of trustworthiness (e.g., safety, resiliency, availability, cybersecurity) differently than IT equipment.
- IoT may be able to replace OT equipment, but the new IoT equipment may offer different or significantly expanded functionality that organizations must consider before replacement.

Questions to consider

1. How should other aspects of trustworthiness (e.g., safety, privacy, resiliency) be considered in addressing cybersecurity?
2. How can organizations manage the discrepancy between expected service life of IT, OT, and IoT systems and system elements?

Emerging Cybersecurity Techniques and Solutions

As approaches and techniques to cybersecurity change, NIST's guidelines must stay relevant and useful. The complexity of IoT applications means different organizations may need to utilize different methods to keep their systems secure. Since the publication of SP 800-213 in 2020, cybersecurity techniques and solutions have emerged and could play a role in securing information systems:

- Zero-Trust Architecture (ZTA) and Continuous Authorization
- Secure IoT On-Boarding and IoT Device Intent Signaling
- Secure Software Development and Cybersecurity Supply Chain Risk Management

NIST has published work in each of these areas. *Zero Trust Architecture*, SP 800-207 details guidelines for organizations to deploy a ZTA in their environments. Further, ZTA practice guides from the NIST National Cybersecurity Center of Excellence (NCCoE) titled *Implementing a Zero Trust Architecture*, SP 1800-35 are in development as a result of a successful NCCoE project demonstrating 19 sample zero trust architecture implementations.

With respect to IoT device intent signaling, an NCCoE project demonstrated and documented the use of the Manufacturer's Usage Description (MUD) to ensure IoT devices send and receive only the traffic required to operate as intended, with the network prohibiting all other communication with the device, thereby increasing the device's resilience to network-based attacks. The builds were documented in *Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)*, SP 1800-15.

The NCCoE has also successfully completed a project demonstrating secure, automated IoT device network-layer on-boarding using five functional technology solutions, as well as two factory provisioning builds. The builds for this project are documented in *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol-Based IoT Device and Network Security*, SP 1800-36, which are on track to be finalized soon.

NIST has also published the *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*, SP 800-218 which documents a core set of high-level secure software development practices that can be integrated by software producers to help reduce the number of vulnerabilities in released software, mitigate the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and address the root causes of vulnerabilities to prevent future recurrences. NIST also published Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, SP 800-161 Rev. 1, which provides guidance to organizations on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of their organizations. The publication integrates cybersecurity supply chain risk management (C-SCRM) into risk management activities. At the

NCCoE a Software Supply Chain and DevOps project is progressing that focuses initially on developing and documenting an applied risk-based approach and recommendations for secure DevOps and software supply chain practices consistent with the SSDF, C-SCRM, and other NIST, government, and industry guidance.

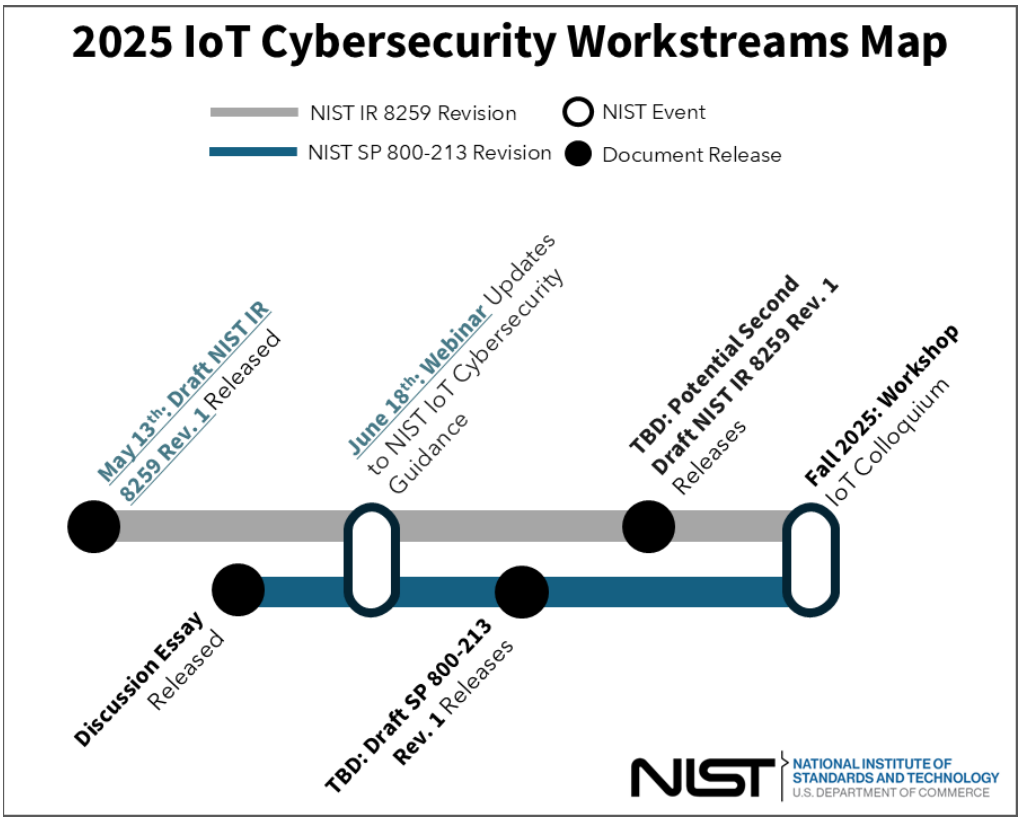
Questions to consider

1. How can a revision of SP 800-213 incorporate these emerging solutions and techniques in the context of IoT products and their deployment?
2. Under what conditions should each of these solutions and techniques be recommended?
3. How can a revision best guide organizations to track and consider nascent and emerging solutions for cybersecurity and other aspects of trustworthiness (e.g., safety, privacy, resiliency), such as privacy enhancing technologies?

Next Steps

In addition to these areas, we welcome your ideas about any topics NIST should consider and other feedback that can help us update NIST SP 800-213! As we kick-off this revision process for SP 800-213, NIST has already initiated a revision of *Foundational Cybersecurity Activities for IoT Device Manufacturers*, NIST 8259, and actively engages with other federal agencies on use-case specific topics. These efforts will proceed in parallel, which will allow for NIST to collect feedback and engage with the community on both documents simultaneously. The Workstreams Map below shows these touch points, as well as previous and prospective document releases. NIST will host a virtual webinar on June 18th to discuss some of these ideas as well as invite questions, feedback, and discussion on potential areas of revision for SP 800-213!

If you can't make the June 18th webinar or have additional thoughts, we encourage you to reach out to the team! Along the way, NIST always welcomes input from the community and can accommodate 1-on-1 meetings, roundtables, or other briefs that would be helpful in stimulating discussion and gathering feedback about our work. If you have an idea or would like to talk with the team, you can drop us a line by July 31st at iotsecurity@nist.gov so NIST has time to consider all feedback for a release of draft SP 800-213 Rev. 1 later in the Summer.


2025 IoT Cybersecurity Workstreams Map
NIST IR 8259 Revision
NIST SP 800-213 Revision
NIST Event
Document Release
May 13th: Draft NIST IR 8259 Rev. 1 Released
June 18th: Webinar Updates to NIST IoT Cybersecurity Guidance
TBD: Potential Second Draft NIST IR 8259 Rev. 1 Releases
Fall 2025: Workshop IoT Colloquium
Discussion Essay Released
TBD: Draft SP 800-213 Rev. 1 Releases
NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE