Discussion Forum: Updates to NIST IoT Cybersecurity Guidance

NIST Cybersecurity for IoT Program

June 18, 2025
1:00pm – 4:00pm ET

Product Disclaimer

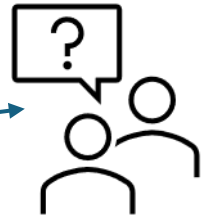
Certain commercial entities, equipment, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Welcome!

Today's Agenda

1. Overview of NIST Cybersecurity for IoT Program Map
2. Review of NIST IR 8259 Revision 1 Draft Changes
   - Draft released on May 13th, comments due by July 14th
3. Presentation of Initial Ideas for a Worked Example of NIST IR 8259
4. Discussion of Potential Topics for NIST SP 800-213 Revision
   - Discussion essay released on June 3rd, comments due by July 30th

Your questions and feedback are always welcome, but when you see this symbol, we want to hear from you!

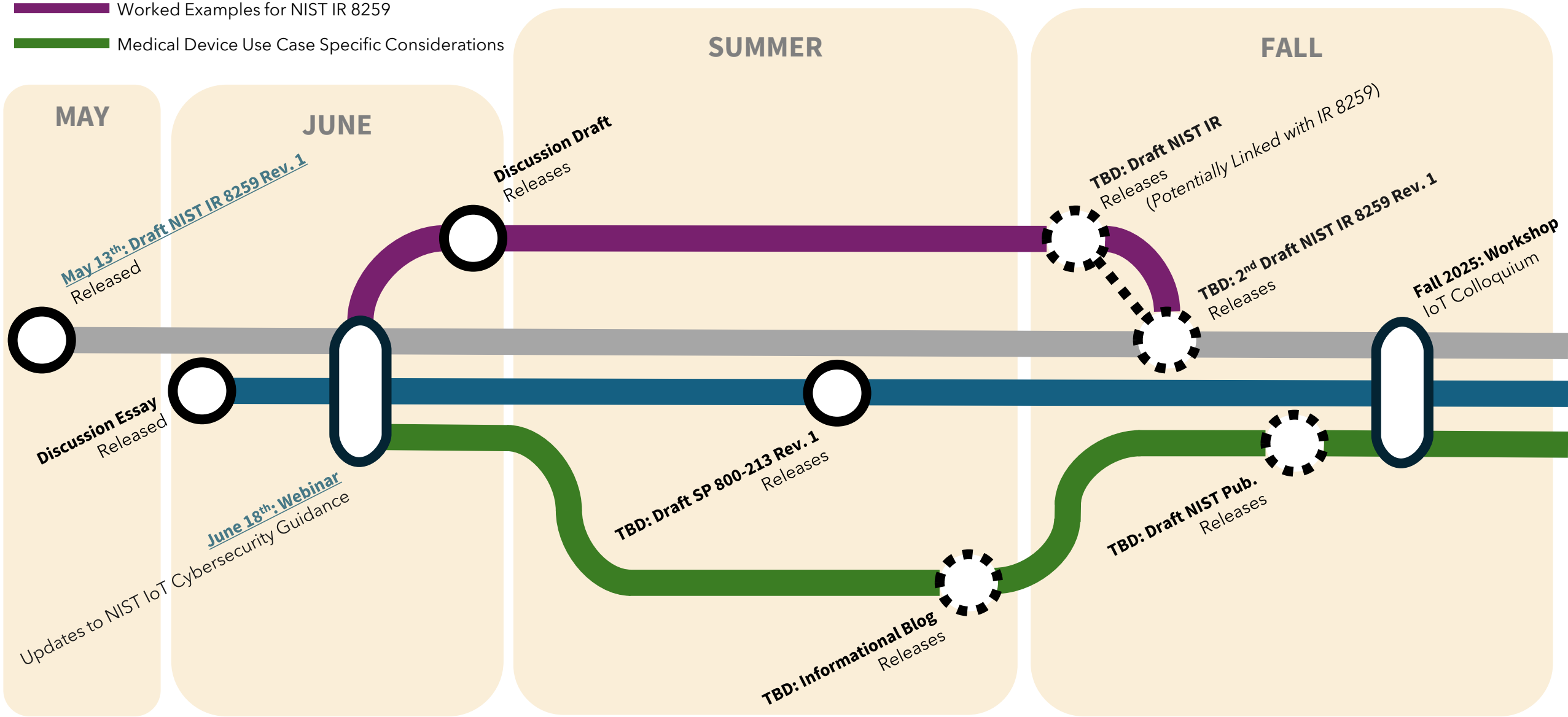


Roadmap for the NIST Cybersecurity for IoT Program

2025 IoT Cybersecurity Workstreams Map

NIST IR 8259 Revision
NIST SP 800-213 Revision
Worked Examples for NIST IR 8259
Medical Device Use Case Specific Considerations
Document Release
Potential Release
NIST Event

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE



NIST IR 8259 Revision 1 Update

Summary Level Changes to NIST IR 8259 Rev 1 IPD

Key Activity Enhancements:

- Added cybersecurity testing questions
- Emphasized customer expectations
- Highlighted post-market update processes
- Noted related privacy considerations

Product Ecosystem Components:

- Defined comprehensive product components
- Added different roles for perspective
- Enhanced risk mitigation strategies
- Added context on IoT threat landscape

Product Cybersecurity Approach:

- Introduced risk-based methodology
- Differentiated "securable" vs "secure" products
- Connected cybersecurity needs and risks
- Cybersecurity of components

Structural Changes:

- Updated graphic figures
- Updated informative references
- Improved document clarity and comprehension

Updates to the Introduction

Executive Summary

- Document updated with revised product scoping language
- Added new section on IoT threat landscape
- Expanded focus on cybersecurity's role in product development

Introduction

- Contextualized IoT growth over past two decades
- Emphasized cybersecurity as key innovation driver

Purpose and Scope

- Clarified difference between 'securable' and 'secure' IoT products
- Provided guidelines for cybersecurity capabilities
- Highlighted how capabilities can be tailored to customer needs

Updates to Section 2. Background

2.1 Product Cybersecurity and System Cybersecurity

- Introduced risk-based approach focusing on entire information system's risks.
- Moved references (informative references will now be published in the Cybersecurity and Privacy Reference Tool [CPRT]).
- Simplified terminology around cybersecurity controls.

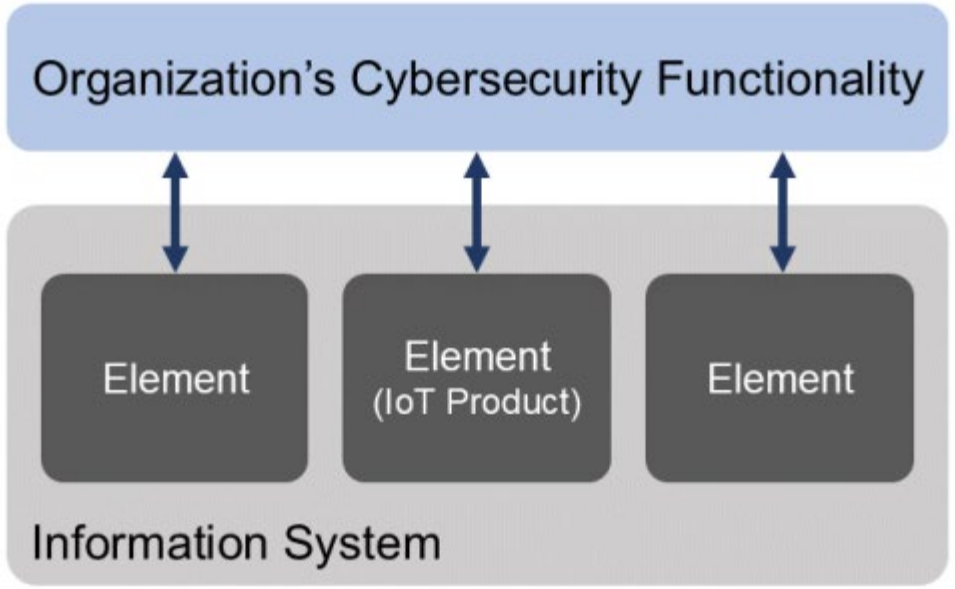


Fig. 1. Relationship of organizational information system elements to an organization's cybersecurity.

Cont. Updates to Section 2. Background

2.2 Composition of IoT Products

- Expanded discussion of IoT product components
- Clarified product architecture variations
- Defined IoT components: device, networking hardware, companion software, backends

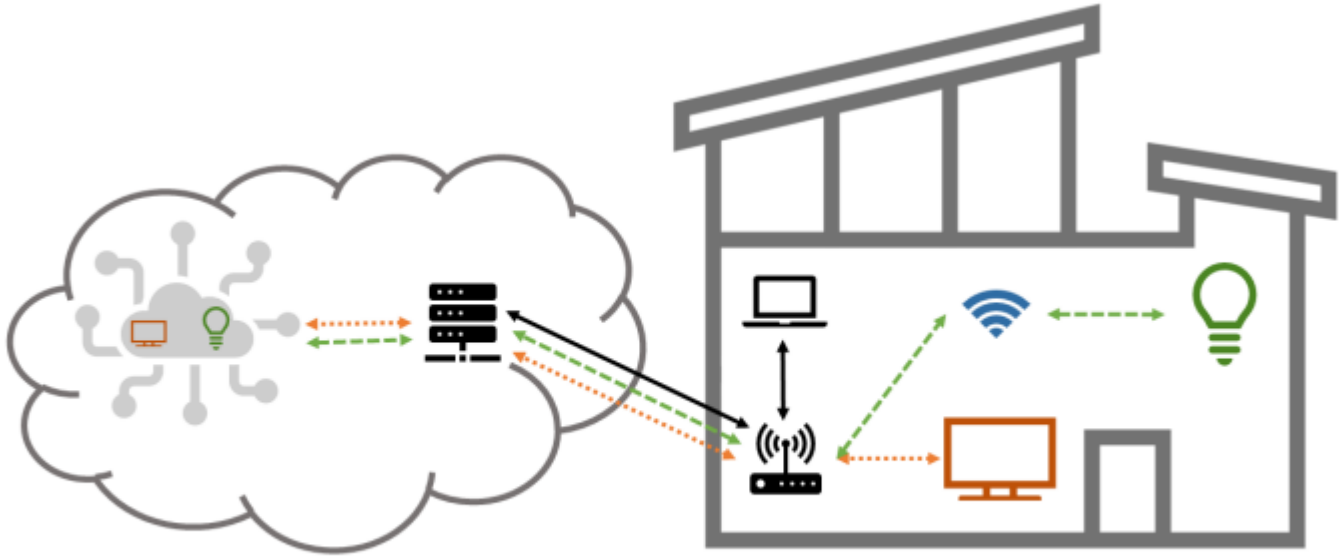


Fig. 2. Example of a network showing multiple IoT products based around different IoT devices which are supported by various kinds of IoT product components.

Cont. Updates to Section 2. Background

2.3 Entities in an IoT Product Ecosystem

Added roles:

- **Supplier** – These entities sell or otherwise provide resources, hardware, software, etc. to other entities.
- **Installer** – These entities deploy hardware, software, etc. into their operational environments.
- **Maintainer** – These entities maintain the hardware and software in the IoT product.

2.5 IoT Product Customer Cybersecurity Need and Goals

- Clarity on enterprise risk mitigation areas.
- Highlighted critical vulnerability management and emphasized temporary mitigation strategies.

Discussion on Questions on Section 2

1. Is the explanation of the scope of the product clear?

2. Are there additional entities that should be considered in Section 2.3 “Entities in an IoT Product Ecosystem?”

Updates to Section 3. Manufacturer Activities Impacting the IoT Product Pre-Market Phase

3. Manufacturer Activities Impacting the IoT Product Pre-Market Phase

- Emphasis up front on determining the operational features and functions of a product

3.1. Activity 1: Identify Expected Customers and Define Expected Use Cases

- Emphasis on environments:

> **4. What digital environments will the product be used in?** (e.g., unmanaged Wi-Fi networks; managed enterprise or industrial networks
>
> **8. How might attackers misuse or compromise the... [*new*] *product in the expected physical and digital environments*?**
>
> **9. What kinds of data will the product create from its sensors or need to actuate on the environment?** (e.g., will create video from a camera, will need location data for weather to adjust thermostat)

Cont. of Updates to 3. Manufacturer Activities Impacting the IoT Product Pre-Market Phase

3.2 Activity 2: Research Customer Cybersecurity Needs and Goals

- What are the known cybersecurity requirements for the IoT product?
    - An example points out the use for multi-factor authentication or zero-trust authentication.
    - A callout box was added on identifying an initial risk assessment.
- For each use case, reasonable threats and how the product may be vulnerable to the threats with what risks may result should be identified.
- An *initial risk assessment* can be performed even if a complete risk assessment cannot.

> An initial risk assessment is distinct from a risk assessment in that an initial risk assessment is performed without full knowledge of deployment environment and cybersecurity expectations. Like with all risk assessments, performance of an initial risk assessment requires understanding of threats, vulnerabilities, etc., but focuses on the threats, vulnerabilities, etc. that can be assumed and expected based on the IoT product's design, components, etc., as well as characteristics ascertainable about the customer, such as their cybersecurity expectations. Sources of information that can be helpful in performing an initial risk assessment include, but are not limited to guidelines from NIST or other organizations, national and international voluntary consensus standards, national and international regulations, and industry best practices.

Cont. of Updates to 3. Manufacturer Activities Impacting the IoT Product Pre-Market Phase

3.3. Activity 3: Determine How to Address Customer Needs and Goals

- Clarified technical means and implementation limitations.
- Added note on customer-controlled security measures.
- Expanded definition of 'robust' security.
- Refined IoT product component descriptions.

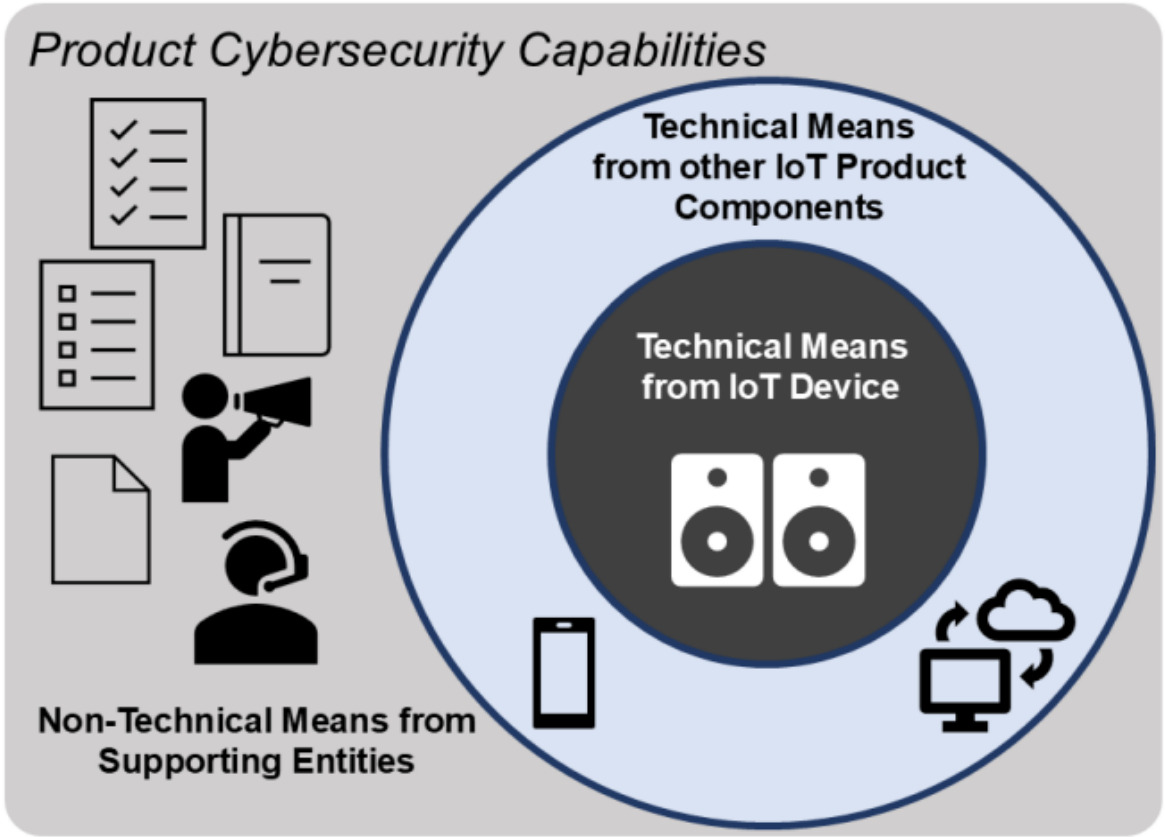


Fig. 6. Technical and non-technical means that can support cybersecurity of IoT products provided as product cybersecurity capabilities.

Cont. of Updates to 3. Manufacturer Activities Impacting the IoT Product Pre-Market Phase

3.4 Activity 4: Plan for Adequate Support of Customer Needs and Goals

- Addition of questions on improving securability of IoT products across components:

1. Which product cybersecurity capabilities are relevant to each IoT product component?
2. How can each relevant product cybersecurity capability be appropriately implemented for each IoT product component?
3. How can cybersecurity be supported within the IoT product boundary?
4. How much control and cybersecurity responsibility will the customers, manufacturer, or other entities have over each IoT product component?
5. How can necessary cybersecurity support be coordinated for all IoT product components, potentially across multiple entities?

- Additional questions to identify secure development practices:

7. What cybersecurity conforming testing or labelling could potential customers look for in IoT products or IoT product components?
8. Which cybersecurity risk were considered in development of the IoT product, what actions, controls, etc. are expected from customers, and how can expectations be effectively communicated?

Discussion on Questions on Section 3

1. Are there additional resources that should be referenced for "initial risk assessment"?

2. Are there additional secure development practices that should be cited in Section 3.4 “Plan for Adequate Support of Customer Needs and Goals?”

Updates to 4. Manufacturer Activities Impacting the IoT Product Post-Market Phase

Under Activity 5: Support Product Cybersecurity through End-of-Life:

- New activity that introduces end-of-life cybersecurity guidelines for IoT devices to help manage cybersecurity risks after a device's lifecycle ends
- Keeping security a priority even after support ends, covering:
  - Secure decommissioning – guidelines for retiring IoT devices safely
  - Data protection – ensuring user data is deleted or transferred securely
  - Customer notifications – informing users when security updates stop

Discussion on Questions on Section 4

1. Do the activities adequately address maintaining cybersecurity through the end-of-life?

2. What additional challenges to long term support need to be more comprehensively considered earlier in the product lifecycle?

Additional Questions or Comments?

- Do the activities adequately reflect the product cybersecurity considerations for a broad range of use cases and customers? Ex:
  - Industrial IoT customers?
  - Consumer IoT?
  - Commercial/Enterprise IoT?
  - Additional IoT sectors to discuss?

- We welcome questions and discussion on the NIST IR 8259 Revision 1 Draft!

NIST IR 8259 Revision 1: Worked Example (in progress)

Worked Example Project Information

Background

- Requests from community to produce a worked example of IoT cybersecurity work.
- Value in using different means to communicate and reinforce concepts.

Purpose and Scope:

- Demonstrate the application of NISTIR 8259 to fictional, but realistic product.
- Explore real-world considerations and challenges.
- Focus on cybersecurity for the example IoT product guided by the activities of NISTIR 8259.

Approach:

- Select and describe a fictional, but realistic IoT product to work as an example.
- Apply each foundational activity from NISTIR 8259 to the example IoT product.
- Report on the information generated by applying the activities and insights gained from the exercise.

Schedule:

- Discuss ideas here today.
- Publish a Discussion Essay following this Webinar.
- Meet with interested stakeholders, gather feedback, and develop the example.
- Publish the Worked Example (likely as part of the NISTIR 8259-series)

Worked Example: Connected Appliance

Manufacturer: Mature in their product development process, but no cybersecurity focus until now.

Customer: Industrial, educational, federal agencies in the U.S.

Product: A commercial-grade dishwasher with network connectivity for remote operation and automated maintenance, performance monitoring, upgrades, data collection.

ILLUSTRATIVE EXAMPLE

Real-world example commercial-grade dishwashers (*provided for visual reference of product form factor*)

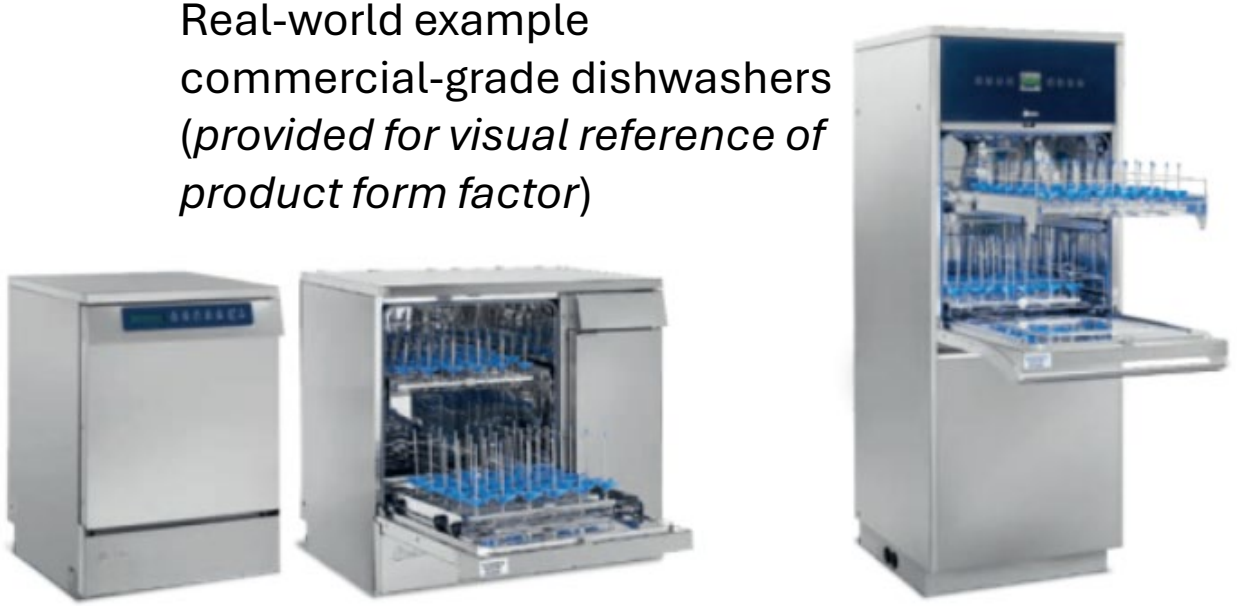


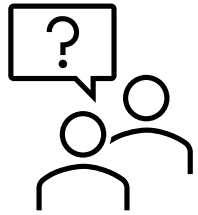
Image: https://labs-usa.com/laboratory-dishwasher/

Activities 1 and 2: Customer Requirements

- Examine different types of requirements and align to different security goals:
  - **Purchasing organization goals**: maximizing device availability, device longevity, encrypting organizational data, authorized access to product functionality, non-technical security goals, security documentation for customer
  - **IT organization goals**: event log collection from all devices, keeping all products patched, configurable security, inventory management
  - **Manufacturer goals**: robust field services, securing intellectual property, reputation of being trustworthy, cost-effective security implementation, adaptable to user environments, supply chain considerations
  - **Post support goals**: Vulnerability disclosure, security patching

ILLUSTRATIVE EXAMPLE

Question: What does your organization struggle with when performing similar activities?

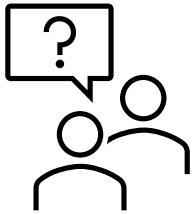


NIST 8259 Activities 3 and 4: SDLC

- Obtaining adequate resources for implementing security during Planning. Prioritizing, allocating trained personnel and allowing adequate time to produce security deliverables
- Secure SDLC: Requirements to Testing phases
- Security Risk Management Process

ILLUSTRATIVE EXAMPLE

Question: What does your organization struggle with when performing similar activities?

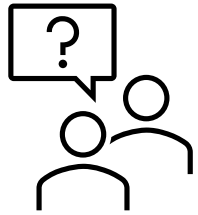


NIST 8259 Activities 5, 6, 7: Post-Market Support

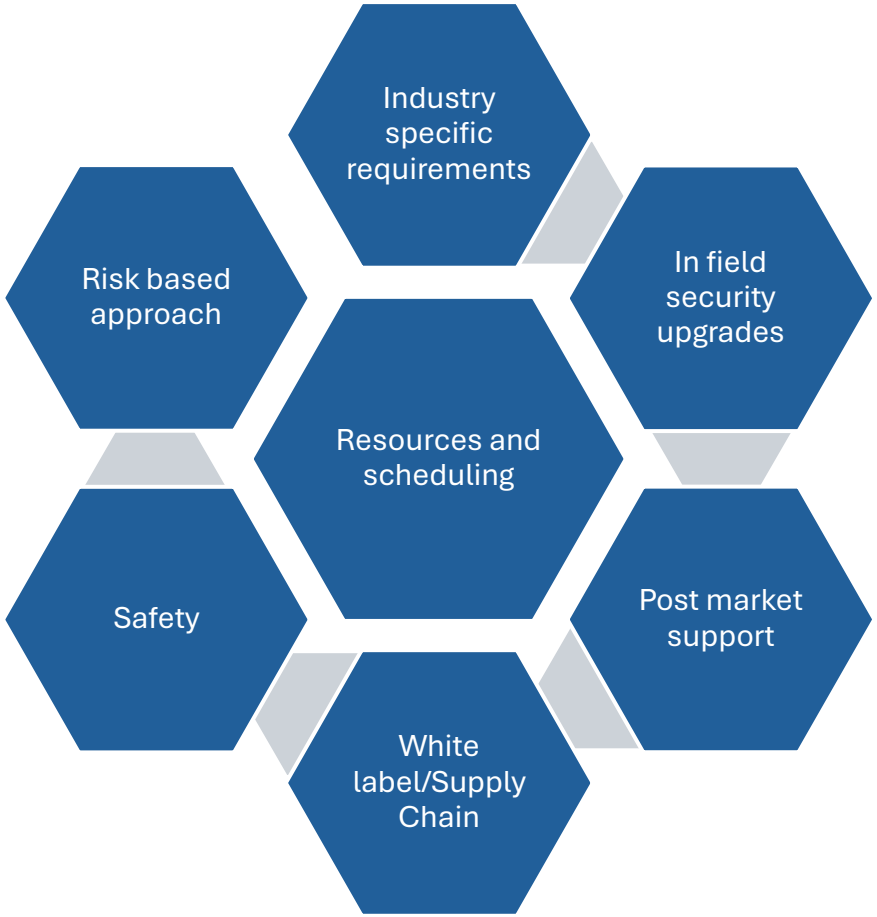
- Vulnerability Monitoring and Disclosure
- Software Bill of Materials (SBOM)
- Incident Investigation Responsibilities
- End of Life activities
- Customer Communication

ILLUSTRATIVE EXAMPLE

Question: Does your organization have additional post-market activities or obligations? If so, which ones?

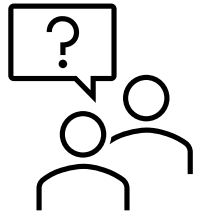


Feedback Needed: Real-life Pain Points?



ILLUSTRATIVE EXAMPLE

Question: What additional examples would anyone like to explore?



NIST SP 800-213 Update

IoT in the Federal Government

- Federal agencies across the government are actively deploying Internet of Things (IoT) technologies to enhance:
  - connectivity,
  - security,
  - environmental monitoring,
  - transportation,
  - healthcare, and
  - industrial automation among many others.

NIST SP 800-213

- NIST looks to our IoT cybersecurity guidelines for federal agencies and other organizations, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*, SP 800-213, which was published in November of 2021.
- Expectation to revisit and, if necessary, revise this work every five years.

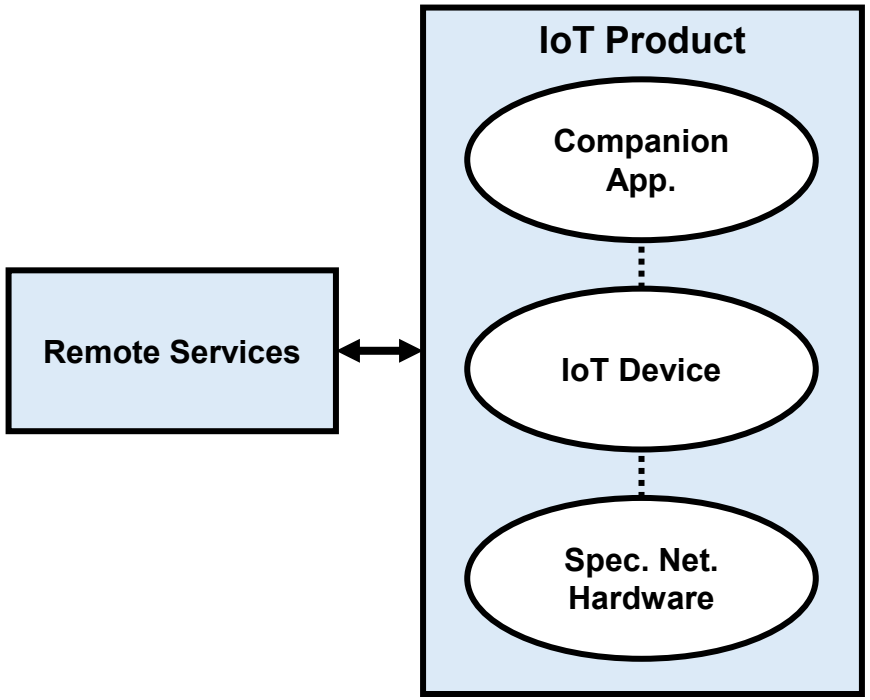
Updates in Process to NIST SP 800-213

- Some example areas of revision for the community to consider while NIST engages and gathers feedback include:
  - IoT Products
  - Emerging Cybersecurity Techniques and Solutions Emerging
  - Convergence between Operational Technology (OT) and Information Technology (IT) via IoT

IoT Products

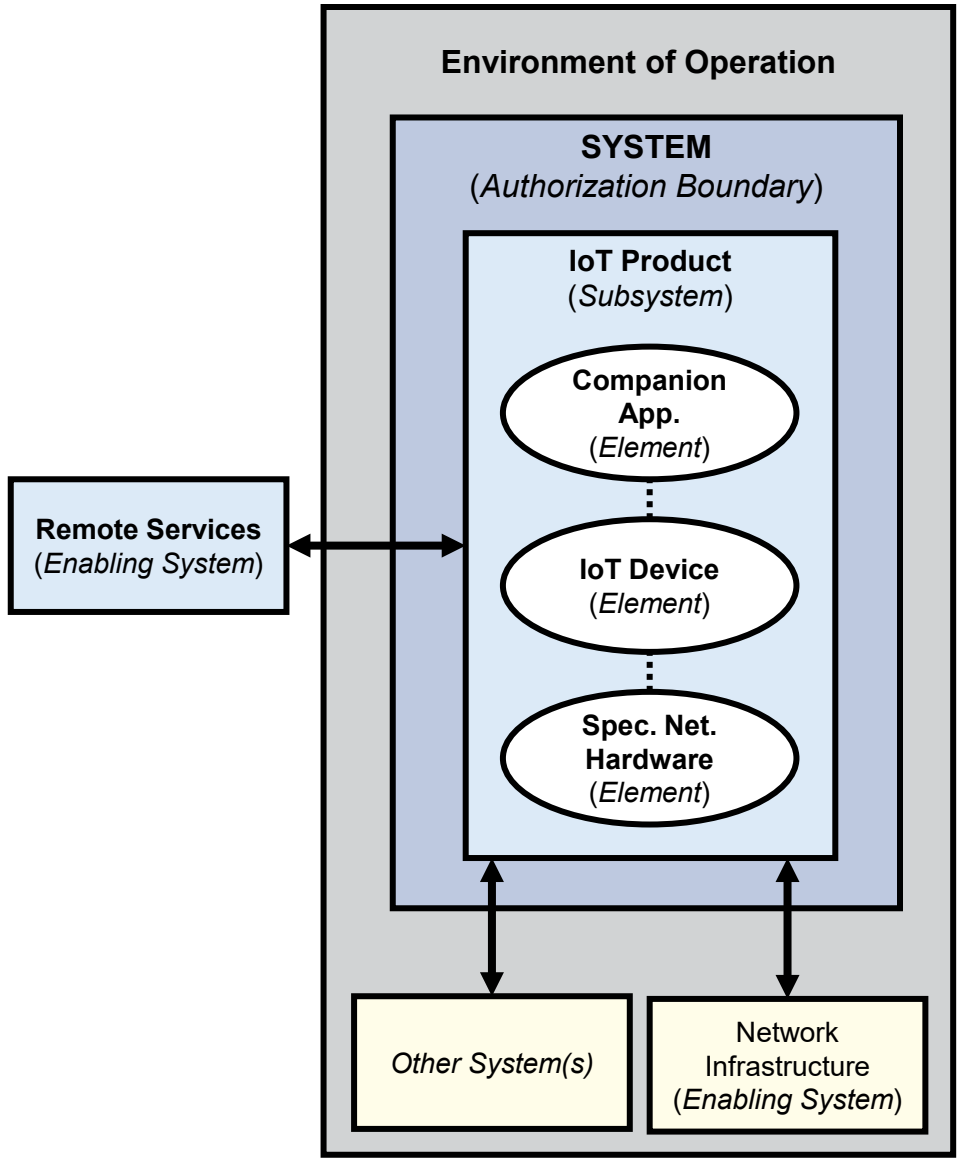
IoT Products in Federal Information Systems (FIS)

- How SP 800-213 can be revised to better address the adoption of IoT *products* by organizations.
- One key consideration is the organization's level of integration expected for the IoT product. We can consider "levels of integration":
  - The IoT product and local components of the IoT product are treated as part of the organization's system.
  - The IoT product is treated as a separate system from the organization's other systems.



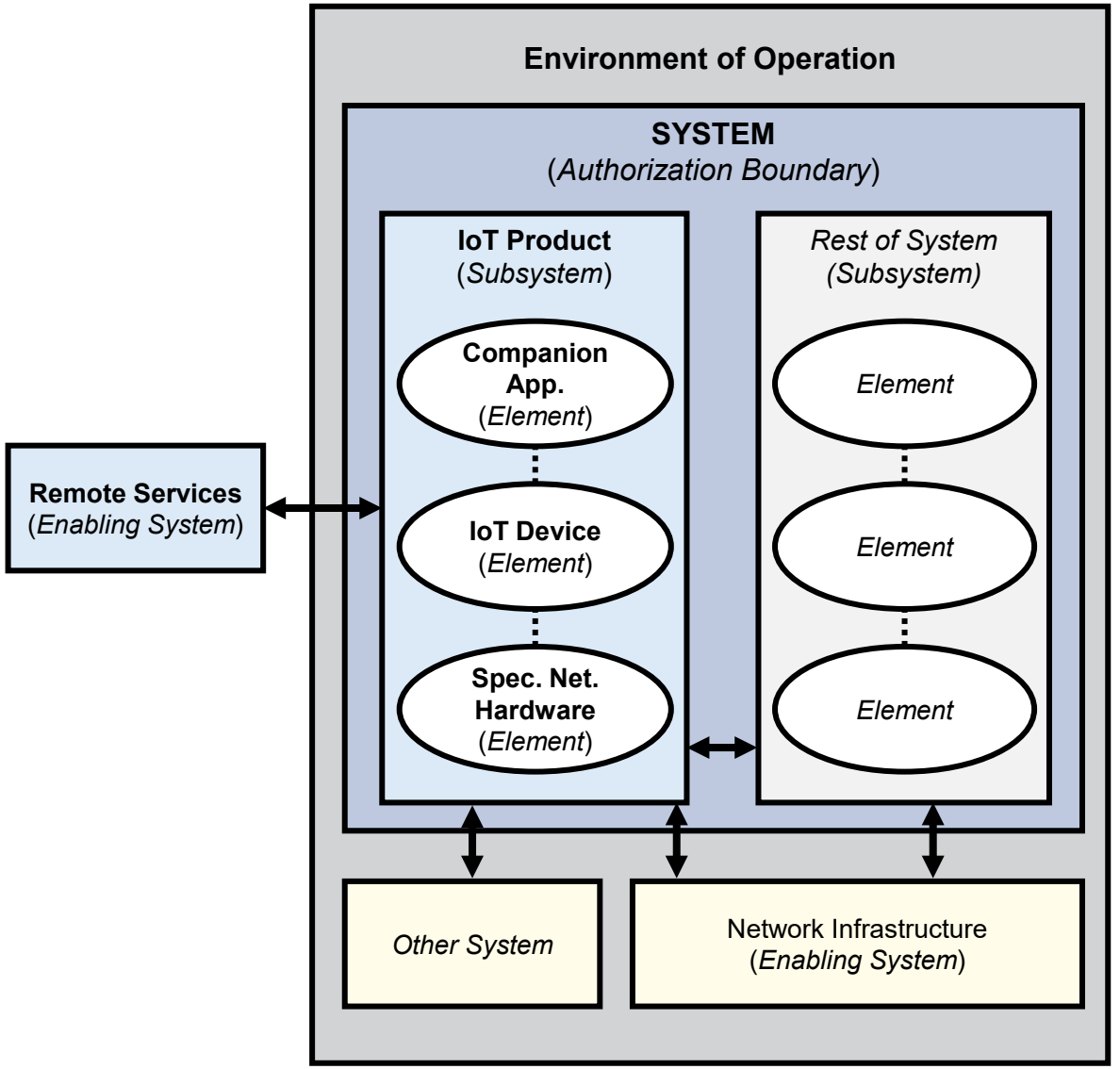
IoT Products in FIS View 1

- An IoT product could be viewed as a new system.
- In this case, IoT Product is a system that will interact with other systems within the environment of operation.
  - *Interacting* with other systems means these interactions should be considered as part of the IoT product system risk assessment.



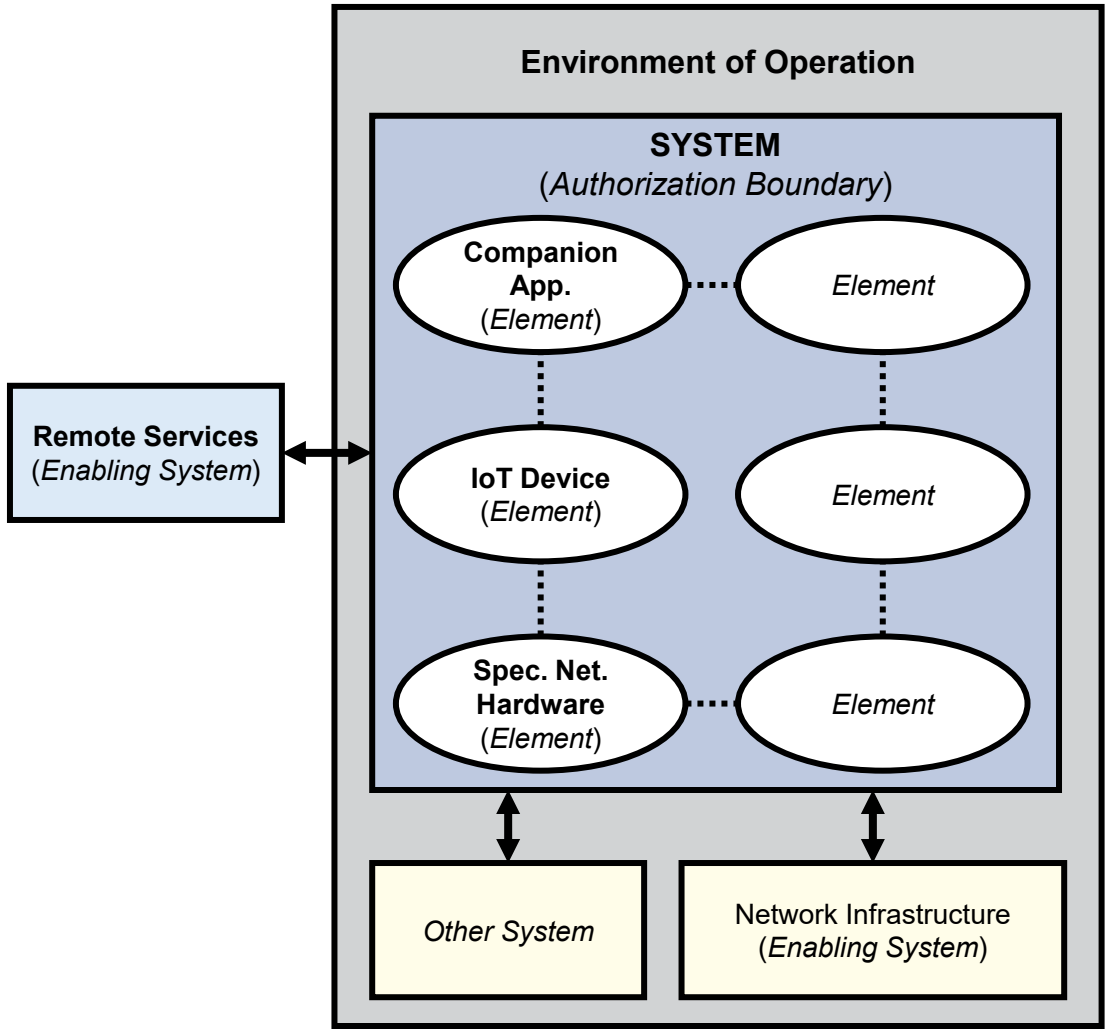
IoT Products in FIS View 2

- An IoT product could be viewed as a sub-system of another system.
- In this case, IoT Product is a sub-system that will integrate with the rest of the system.
  - *Integrating* means the IoT product should be considered when assessing the risks the system faces.



IoT Products in FIS View 3

- An IoT product could be viewed as part of the system, with locally deployed IoT product components treated as individual elements of the system.
- In this case, IoT Product's local components are considered elements of the system, while as before, remote components are considered enabling systems.



IoT Products in FIS Other Considerations

- 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?

Questions to Consider:

1. How should NIST discuss IoT devices that rely on other components to operate in SP 800-213?
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 software and remote services IoT product components?

Emerging Cybersecurity Techniques and Solutions

Emerging Cybersecurity Techniques and Solutions

- 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 Publications on Zero Trust Architectures

- *Zero Trust Architecture*, SP 800-207
  - Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned).
  - Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established.
- *Implementing a Zero Trust Architecture*, SP 1800-35
  - The NCCoE worked with 24 collaborators to build 19 ZTA example implementations and demonstrate a number of common use cases.

NIST Publications on Emerging Cybersecurity Techniques and Solutions for IoT

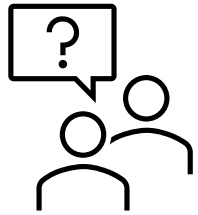
- *Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)*, SP 1800-15
  - MUD provides a standard way for manufacturers to indicate the network communications that a device requires to perform its intended function.
  - When MUD is used, the network can automatically permit the IoT device to send and receive only the traffic it requires to perform as intended, and the network can prohibit all other communication with the device.
- *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol-Based IoT Device and Network Security*, SP 1800-36
  - This guide shows how to provide network credentials to IoT devices in a trusted manner and maintain a secure device posture throughout the device lifecycle.

NIST Publications on Development and Supply Chain Cybersecurity

- *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*, SP 800-218
  - This document recommends a core set of high-level secure software development practices that can be integrated into each SDLC implementation.
  - Following these practices should help software producers 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.
- *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, SP 800-161 Rev. 1
  - This publication provides guidance to organizations on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of their organizations.
- A Software Supply Chain and DevOps project is progressing at the National Cybersecurity Center of Excellence (NCCoE)

Questions to Consider:

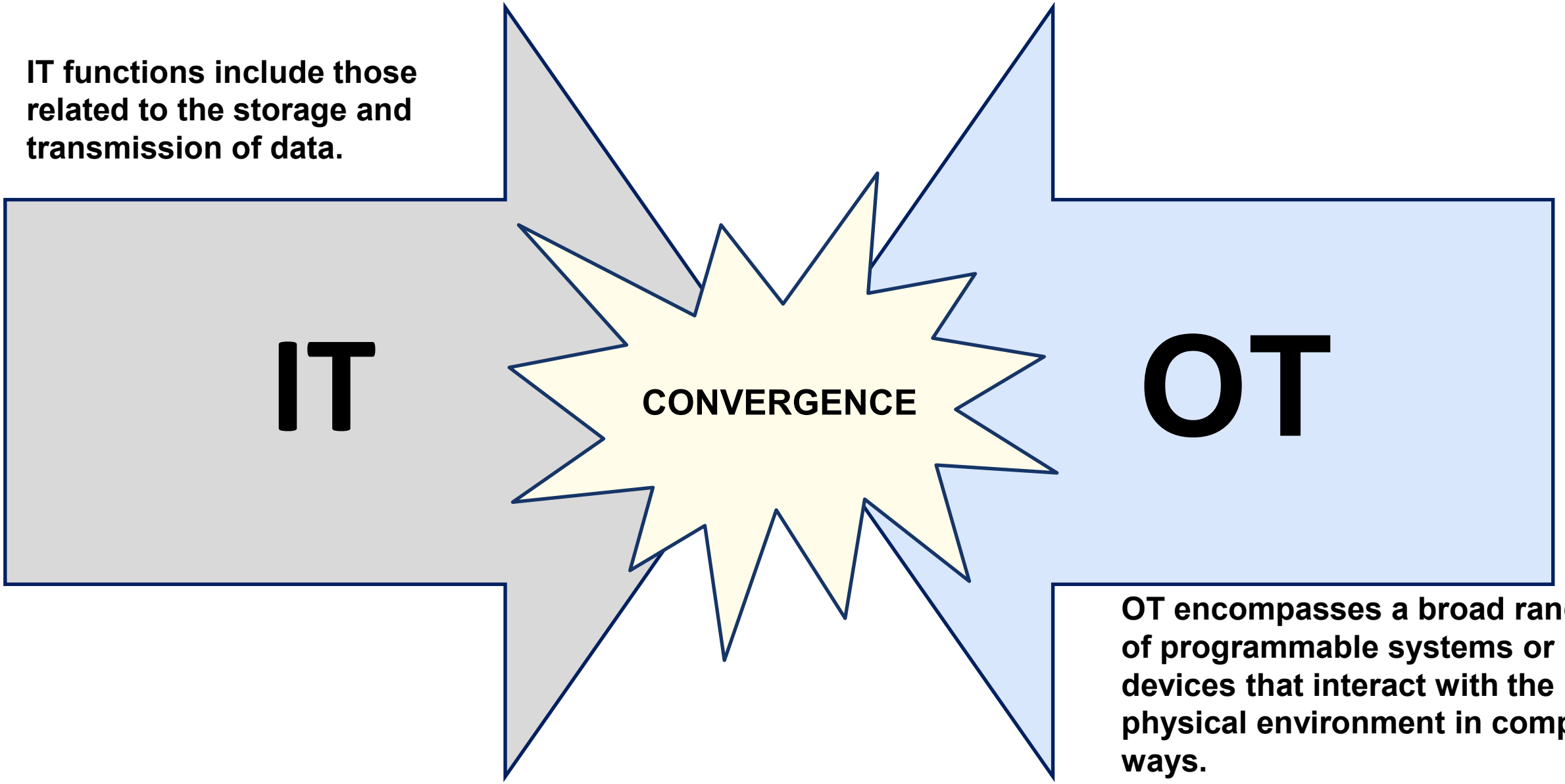
1. How can a revision of SP 800-213 incorporate these emerging solutions and techniques in the context of IoT products and their deployment?
2. Under what conditions should each of these solutions and techniques be recommended?
3. How can a revision best guide organizations to track and consider nascent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



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

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

IT functions include those related to the storage and transmission of data.



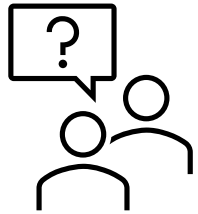
OT encompasses a broad range of programmable systems or devices that interact with the physical environment in complex ways.

Challenges with OT Systems and Convergence

OT SYSTEMS	CONVERGENCE
• OT systems and devices often have long service lives. • OT systems may be deployed in hard-to-reach locations (e.g., embedded in walls of buildings) • OT systems perform functions that were previously stand alone or only available on local networks.	• OT equipment may use networking technologies (e.g., ethernet, Wi-Fi), but were not originally intended to connect to the internet. • OT or IoT equipment may need to balance multiple aspects of trustworthiness (e.g., safety, resiliency, availability, cybersecurity). • New IoT equipment may offer different or significantly expanded functionality that changes cybersecurity considerations.

Questions to Consider:

1. How should other aspects of trustworthiness (e.g., safety, resiliency, availability) 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?



Feedback and Comments are Welcome!

- **By July 14**, please provide your comments on the NIST IR 8259 Rev.1 Initial Public Draft (IPD) draft revision that was published on May 14, 2025: https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8259r1.ipd.pdf

- **By July 31**, please provide your comments on the 800-213 discussion essay, which presents some example areas of revision for the community to consider: Essay Update to 800-213 2025-06-03.pdf

As always, NIST welcomes feedback and discussion from the community!
You can send comments to: iotsecurity@nist.gov

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

THANK YOU

CONTACT US

NIST.gov/cybersecurity @NISTcyber

NIST Cybersecurity for IoT Program Home Page