NIST IoT Morning Coffee Session for Forum Members

Overview of SP 800-213 / 213A: IoT Device Cybersecurity Guidance for the Federal Government

Cybersecurity for IoT Program, NIST
May 17th, 2022
A Working Definition of IoT

At least one **transducer** for interacting directly with the **physical world**
(e.g., a sensor or actuator)

&

At least one **network interface** for interfacing with the **digital world**
(e.g., Ethernet, Wi-Fi, Bluetooth, Long-Term Evolution [LTE], Zigbee, Ultra-Wideband [UWB])

This definition is utilized in U.S. Public Law 116-207, IoT Cybersecurity Improvement Act of 2020
IoT Potentially Introduces Unique Risks Into An Information System Environment

Looking through the prism of what is different about IoT:
1. Device Interactions with the Physical World
2. Device Access, Management, and Monitoring Features
3. Cybersecurity and Privacy Capability Availability, Efficiency, and Effectiveness

NIST identified 11 areas of cybersecurity and privacy risk management that will likely be impacted as organizations adopt IoT technologies (NISTIR 8228)
NIST Has Developed Broadly Applicable IoT Cybersecurity Guidance

NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

Guidance for Manufacturers

- NISTIR 8259: Foundational Activities for IoT Device Manufacturers
- NISTIR 8259A: Technical Core Baseline
- NISTIR 8259B: Non-Technical Core Baseline

Guidance for Federal Agencies

- SP 800-213: Establishing IoT Device Cybersecurity Requirements
- SP 800-213A: IoT Device Cybersecurity Requirement Catalog

Protect Device Security

Protect Data Security

Protect Individuals’ Privacy
Our IoT Device Guidance Aligns With The RMF, Providing Process and Specific Controls

Risk Management Framework

- Life Cycle Approach
  - SP 800-37r2
- Security & Privacy Controls
  - SP 800-53r5

- IoT Device Cybersecurity Requirements Development
  - SP 800-213
- IoT Device Cybersecurity Requirement Catalog
  - SP 800-213A
The SP 800-213 Process Links IoT Cybersecurity to the RMF

3.1 Important IoT Device Security Considerations

3.2 Assessing Risk and Determining Required Security Controls

3.3 Identifying Device Cybersecurity Requirements

Risk Assessment of the System

FEDERAL SYSTEM
(Authorization Boundary)

Element (IoT Device)

Element

Element

- Identify Effects of IoT Device on Threat Sources and Events
- Identify Effects of IoT Device on Vulnerabilities and Predisposing Conditions
- Identify Effects of IoT Device on Likelihood(s) of Impact
- Identify Effects of IoT Device on Magnitude(s) of Impact

Determine Updated Risk Assessment
The SP 800-213A Catalog Details IoT Device Cybersecurity Requirements of Two Types

- Device Cybersecurity Requirements
- Non-Technical Supporting Requirements

- Cybersecurity Framework Mapping
- SP 800-53r5 Security Controls Catalog Mapping
- Federal Profile of IoT Cybersecurity Requirements

- Low Impact Baseline

SP 800-53B Control Baselines
The Roles of SP 800-213 & SP 800-213A

SP 800-213: Determining Requirements
- Relationship to Risk Management Framework Process
- Evaluating IoT Device Risk
- Selecting Requirements

SP 800-213A: Capabilities Catalog
- Builds from NISTIR 8259A/B Baselines
- Detailed Technical & Supporting Capabilities

Webinar Objective: Provide an Overview of These Two Documents And Relate Them To Other NIST Guidance
IoT Devices are System Elements

• Built by manufacturers
• Integrated into federal information systems
• Integral piece of overall risk management challenge
• Ideally support security controls “out of the box”
• Management of risk may require new controls or other risk mitigations
IoT Devices Can Introduce Unique Risks

• NISTIR 8228 explored particular risk considerations for IoT devices, relative to traditional IT products, due to
  • Device interaction with the physical world
  • Limited management and monitoring features
  • Cybersecurity and privacy protection shortcomings

• Federal agencies must address unique risks when applying the Risk Management Framework process to systems with IoT device elements
• Organizational security requirements are derived from many areas
• They are satisfied by security capabilities, which consider organizational and system security
• IoT devices, as a system component, may have to support security capabilities
SP 800-213 Defines a 3-Step Process For Establishing IoT Device Cybersecurity Requirements

1. **Understand IoT Device Use Case and Cybersecurity Characteristics**
   - Use case & Benefits
   - Data implications
     - Collection
     - Storage
     - Transfer
   - Interactions with other system elements
   - Manufacturer practices

2. **Understand IoT Device Impacts to System Risk Assessment**
   - Threat source effects
     - Vulnerability effects
     - Likelihood effects
     - Impact effects

3. **Determine Required IoT Device Cybersecurity Characteristics**
   - Apply mapping and profiles
   - Select from other resources
     - NISTIR 8259 A/B
     - NIST SP 800-213A Catalog
     - NIST SP 800-53 Controls
     - NIST Cybersecurity Framework

3.1 **Important IoT Device Security Considerations**
3.2 **Assessing Risk and Determining Required Security Controls**
3.3 **Identifying Device Cybersecurity Requirements**
Consider the IoT Device Use Case and Cybersecurity Requirements

Understand IoT Device Use Case and Cybersecurity Characteristics

- Use case & Benefits
- Data implications
  - Collection
  - Storage
  - Transfer
- Interactions with other system elements
- Manufacturer practices

3.1 Important IoT Device Security Considerations

- IoT Device: How utilized? Benefits?
- Data: What data collected? Storage? Transmission?
- Associated vulnerabilities and risks?
- Support for purchaser’s key device cybersecurity requirements?
- Device manufacturer secure development and maintenance practices (e.g., vulnerability disclosure and remediation)?
Understand the IoT Device Impacts To System Risk Assessment

• How Does The IoT Device Affect:
  • Sources of System Threats?
  • System Vulnerabilities?
  • Likelihood of Threats?
  • Impacts of Threat Actions?

Understand IoT Device Impacts to System Risk Assessment

• Threat source effects
• Vulnerability effects
• Likelihood effects
• Impact effects

3.2 Assessing Risk and Determining Required Security Controls
• Risk assessment considers the entire system
• IoT devices as system elements can impact that risk assessment
• Device impacts may have related impact on appropriate system security measures
A risk assessment considers:
- Threat Sources and Events
- Vulnerabilities and Predisposing Conditions
- Likelihood and Magnitude of Impact

Relative to the entire system, an IoT device may be the same or different related to these considerations.
Determine the Required IoT Device Cybersecurity Characteristics

- Respond to Organizational and System Security Requirements
- Account for IoT-Unique Considerations
- Draw on Established Security Requirements Sources
  - NIST Guidance (for Federal Applications)
  - International Standards
  - Industry Guidance

Determine Required IoT Device Cybersecurity Characteristics
- Apply mapping and profiles
- Select from other resources
  - NISTIR 8259 A/B
  - NIST SP 800-213A Catalog
  - NIST SP 800-53 Controls
  - NIST Cybersecurity Framework

3.3 Identifying Device Cybersecurity Requirements
The SP 800-213A Catalog Details IoT Device Cybersecurity Requirements of Two Types

Device Cybersecurity Requirements

- Device Cybersecurity Capabilities
  - Device Identification
  - Device Configuration
  - Data Protection
  - Logical Access to Interfaces
  - Software Update
  - Cybersecurity State Awareness
  - Device Security

- Non-Technical Supporting Capabilities
  - Documentation
  - Information and Query Reception
  - Information Dissemination
  - Education and Awareness

Technical support is built into the IoT device (i.e., in its own hardware and software).

Non-technical support comes from the IoT device manufacturer or supporting third-parties.
Information about the IoT device, organizational context, and updates to the risk assessment is combined by the organization.

IoT device cybersecurity requirements must support system and organization security capabilities (e.g., security controls).
• Possible no available IoT device addresses all identified cybersecurity requirements

• Organizations can consider options for using devices that fall short

• Must consider risks, benefits to the organization and other factors.
SP 800-213A: IoT Device Cybersecurity Requirement Catalog
SP 800-213A Expands on NISTIR 8259 A/B Baselines

- NISTIR 8259A defines technical capabilities to be *provided* by IoT devices
- NISTIR 8259B defines non-technical supporting activities to be *performed* by device manufacturers (and supporting third parties)
- IoT device cybersecurity is dependent on both types of capabilities
- SP 800-213A provides a catalog of specific capabilities and actions to implement NISTIRs 8259 A & B
- Catalog contents are mapped to SP 800-53r5 and the Cybersecurity Framework v1.1
### Capability Naming in SP 800-213A

- **Capabilities & Sub-capabilities** have names and shorthands:
  - **DI** – Device Identification
  - **IMS** – Identifier Management Support
  - **AID** – Actions Based on Device Identity
  - **PID** – Physical Identifiers

- Supporting requirements have number and letter code

- Mappings to SP 800-53 and Cybersecurity Framework use complete identifiers:
  - SP 800-53 IA-3 & IA-4 map to **DI:IMS(1, 2, 3)**

*Example Mapping*
## Device Cybersecurity Capability Catalog Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Identification (DI)</td>
<td></td>
</tr>
<tr>
<td>Device Configuration (DC)</td>
<td></td>
</tr>
<tr>
<td>Data Protection (DP)</td>
<td></td>
</tr>
<tr>
<td>Logical Access to Interfaces (LA)</td>
<td></td>
</tr>
<tr>
<td>Software Update (SU)</td>
<td></td>
</tr>
<tr>
<td>Cybersecurity State Awareness (CS)</td>
<td></td>
</tr>
<tr>
<td>Device Security (DS)</td>
<td></td>
</tr>
<tr>
<td>Documentation (DO)</td>
<td></td>
</tr>
<tr>
<td>Information &amp; Query Reception (IQ)</td>
<td></td>
</tr>
<tr>
<td>Information Dissemination (ID)</td>
<td></td>
</tr>
<tr>
<td>Education &amp; Awareness (EA)</td>
<td></td>
</tr>
</tbody>
</table>
Presentation of Capabilities in SP 800-213A: A Device Capability Example

CS - CYBERSECURITY STATE AWARENESS

**Description:** The capability to generate data indicating different types of events related to the use of the device to meet organizational requirements.

**Discussion:** Cybersecurity state awareness supports vulnerability management and incident detection by helping enable investigation of compromises, identify misuse, and troubleshoot some operational problems. Capture of cybersecurity state information, logging of this information, and auditing of logs may be needed on the IoT device depending on its design, use case, and other considerations. Cybersecurity state awareness can be critical to ensuring trust in the device’s operation, including device cybersecurity capabilities.

**Sub-Capabilities that may be necessary:**

(AEI) **Access to Event Information**

**Description:** Ability to access IoT device state information.

**Discussion:** Organizations may have various uses for IoT device cybersecurity state information which may require the device to collect and make such data available when necessary.

**Related SP 800-53 Rev. 5 Controls:** SI-4, AU-11, AU-12

**Requirements that may be necessary:**

1. Ability to access information about the IoT device's cybersecurity state and other necessary data.
2. Ability to preserve system state information.

**Mapping to SP 800-53 Rev. 5 Controls that Sub-Capability may support**

**Specific Requirement Statements Related to Sub-Capability**
ID - INFORMATION DISSEMINATION

Description: The ability for the manufacturer and/or supporting entity to broadcast and distribute information related to cybersecurity of the IoT device.

Discussion: Organizations will want to stay informed about the cybersecurity of IoT devices to allow them to fine tune their mitigations and maintain an adequate level of risk assurance. Organizations may need to know ...

Sub-Capabilities that may be necessary:

(CRI) Cybersecurity Related Information Alert

Description: The procedures to support the ability for the manufacturer and/or supporting entity to alert customers about cybersecurity relevant information.

Discussion: This sub-capability supports on-going cybersecurity of the device by keeping customers informed of developments and new information after the initial documentation was developed and provided. Organizations may need to be informed about cybersecurity-related activities on the IoT device, especially if the IoT device is critical to ...


Requirements that may be necessary:

1. Establish communications with the details necessary for maintaining IoT device data integrity during software modifications. Information that may be necessary to provide about maintaining data integrity during software modifications include details and actions such as: ...
A Federal Profile is Included in SP 800-213A

Profiles tailor the IoT cybersecurity guidance to particular market sectors, verticals, or use cases

<table>
<thead>
<tr>
<th>Sub-Capability (requirements)</th>
<th>Possible SP 800-53 Rev. 5 Controls Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Identity (DI)</strong></td>
<td></td>
</tr>
<tr>
<td>Identifier Management Support (IMS)</td>
<td>IA-3, IA-4</td>
</tr>
<tr>
<td>(1) (3)</td>
<td></td>
</tr>
<tr>
<td>Actions Based on Device Identity (AID)</td>
<td>IA-3, AC-3, SI-4, AU-2, CM-8</td>
</tr>
<tr>
<td>(2) (3) (4)</td>
<td></td>
</tr>
<tr>
<td><strong>Device Configuration (DC)</strong></td>
<td></td>
</tr>
<tr>
<td>Logical Access Privilege Configuration (PRV)</td>
<td>AC-3, CM-5</td>
</tr>
<tr>
<td><em>(sub-capability does not list specific requirements)</em></td>
<td></td>
</tr>
<tr>
<td>Authentication and Authorization Configuration (AUT)</td>
<td>AC-3, CM-5</td>
</tr>
<tr>
<td><em>(sub-capability does not list specific requirements)</em></td>
<td></td>
</tr>
<tr>
<td>Interface Configuration (INT)</td>
<td>AC-3, CM-5</td>
</tr>
<tr>
<td><em>(sub-capability does not list specific requirements)</em></td>
<td></td>
</tr>
<tr>
<td>Display Configuration (DSP)</td>
<td>AC-8, AC-12(2), AC-12(3)</td>
</tr>
<tr>
<td><em>(sub-capability does not list specific requirements)</em></td>
<td></td>
</tr>
<tr>
<td>Device Configuration Control (CTL)</td>
<td>CM-2, CM-3, CM-5, CM-6, SR-11(2)</td>
</tr>
<tr>
<td><em>(all requirements)</em></td>
<td></td>
</tr>
</tbody>
</table>
Profiles are possible for many markets or product types

NISTIR 8259A
Technical Core Baseline

NISTIR 8259B
Non-Technical Core Baseline

SP 800-213A
IoT Device Cybersecurity
Requirement Catalog

Other Standards
e.g., ETSI EN 303 645,
ANSI/CTA-2088

Select / Tailor

Core IoT Cybersecurity Capabilities Baseline
NISTIR 8259A / 8259B
In conclusion ... 

- Understand the device(s)
- Understand the risk impacts
- Determine your IoT cybersecurity requirements
- SP 800-213 defines the process
- SP 800-213A catalogs requirements
Have a question or an idea? We want to hear from you!
We’re always accepting thoughtful feedback at iotsecurity@nist.gov.

Further Reading:


Other Cybersecurity for IoT Program Publications - https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/publications

More at our website - https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program