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

# Workshop on Foundational Cybersecurity Activities for IoT Device Manufacturers

NIST Cybersecurity for IoT Program

March 5, 2025

# Welcome!

Katerina Megas

Program Manager, Cybersecurity for IoT Program

# Today’s Agenda (Morning)

- 8:30 - 9:00 AM Registration/Check-in
- 9:00 – 9:15 AM Welcome (Katerina Megas)
- 9:15 – 10:00 AM Morning Keynote Presentation (Jon Boulos, Kimberly-Clark)
- 10:00 – 10:45 AM IR 8259 Rev. 1 Preliminary Update: Overview (Mike Fagan)
- 10:45 – 11:00 AM Break
- 11:00 – 11:55 AM IR 8259 Rev. 1 Preliminary Update: Session 1 (Mike Fagan)
- 11:55 AM – 1:00 PM Lunch Break

# Today's Agenda (Afternoon)

- 11:55 AM – 1:00 PM Lunch Break
- 1:00 – 1:45 PM Afternoon Keynote Presentation (Brad Goodman, Dell)
- 1:45 – 2:45 PM IR 8259 Rev. 1 Preliminary Update:  Session 2 (Mike Fagan)
- 2:45 – 3:00 Break
- 3:00 -3:45 PM IR 8259 Rev. 1 Preliminary Update:  Session 3 (Mike Fagan)
- 3:45 – 4:00 PM Closing Remarks (Mike Fagan)

# Fortifying the Future: Enhancing IoT Security Frameworks

Jon Boulos

Kimberly-Clark

# NIST IR 8259 Revision 1 Preliminary Update:  Overview

Mike Fagan

Technical Lead, Cybersecurity for IoT Program

# Discussion Points from Last Workshop

- Shift the discussion from a focus on IoT devices to IoT products
- Additional discussion of risk assessment/threat modeling
- Should we consider privacy?
  - How?
- Additional post market considerations such as:
  - Maintenance and end-of-life

# Summary of Changes

- Changes made throughout the document to move from consideration of only IoT devices to the broader concept of IoT products. This includes changes in general from device cybersecurity capabilities to product cybersecurity capabilities.
- Additional content in the Background section connecting the concept of cybersecurity needs and goals with cybersecurity risks. This included a deeper exploration of system cybersecurity relative to product cybersecurity.
- Adjustments based on feedback to highlight risk, make better connections with privacy via data security considerations, and to highlight the actionability of post-market communications.
- When the core baseline is mentioned, NISTIR 8259B is added. Also added references where appropriate to SPs 800-213 and 800-213A.
- Made edits throughout the document to improve clarity of presentation such as removing or rewording redundant or confusing phrases, and adding or changing examples given.

# Working Definitions for IoT Products & Devices

An **IoT product** is an **IoT device** and any additional product components that are **necessary** to using the IoT device **beyond basic operational features**.

*NIST IR 8425*

An **IoT device** has…

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,…)

*NIST IR 8259*

The IR 8259 IoT Device definition is utilized in U.S. Public Law 116-207, IoT Cybersecurity Improvement Act of 2020

# Additional Risk Background Added

- Risk is defined as “a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.” [800-37]
    - “those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.” [800-37]
- A risk-based approach to determine cybersecurity controls, which are “the safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.” [800-53r5]
- Dependencies must be met by system components for cybersecurity controls to be feasible or effective.
    - For example, how can access control be enforced if a device on the network does not allow a default password to be changed?

# What role does risk have in product cybersecurity?

- IoT products will have cybersecurity capabilities to support the cybersecurity of the networks to which they are eventually attached.
  - A capability is “a combination of mutually reinforcing controls implemented by technical means, physical means, and procedural means.” [800-37r2]
- More specifically, IoT product cybersecurity capabilities are capabilities as defined above, but provided by or related to the IoT product.
  - IoT device cybersecurity capabilities are capabilities provided by the IoT device specifically (i.e., cybersecurity features or functions the device provides through its own technical means).
  - Other IoT product components may also contribute to IoT product cybersecurity capabilities through their technical means.
  - IoT product non-technical supporting capabilities are procedural means implemented and provided by IoT product manufacturers or other supporting entities that help support cybersecurity.

# Next Steps

- Gathering feedback on preliminary edits
- Working on potential additional updates:
  1. Based on feedback and comments we receive
  2. Related to risk and process(es) manufactures can use
  3. On post-market activities, including potentially additional post-market activities
  4. Drawing more attention to operational, functional, and data considerations to highlight **touch-points** for other aspects of trustworthiness besides cybersecurity
     - No plans to directly address other aspects of trustworthiness (e.g., privacy)
- Will release a Draft for Public Comment

# 15 Minute Break

# NIST IR 8259 Revision 1 Preliminary Update:  Session 1

Mike Fagan

Technical Lead, Cybersecurity for IoT Program

# Activity 1: Identify Expected Customers and Define Expected Use Cases

**Identifying expected customers:**

- For an IoT product is crucial for understanding which cybersecurity features to implement.
- Customers are individuals or organizations who purchase and deploy the product. They often act as administrators for cybersecurity purposes.
- Customers may also be users of the IoT products they purchase.
- Besides primary customers, some IoT products may have additional users who interact with the device but did not purchase it. These users may also have cybersecurity needs and goals.

**Defining expected use cases:**

- Manufacturers should establish expected use cases for the IoT device based on the anticipated customers.
- This helps guide how the product will be reasonably deployed and used.

# Activity 1: Identify Expected Customers and Define Expected Use Cases

**Identify the Expected Customers:**

1. Who are expected customers for this product?
2. What types of organizations are expected customers for this product?

**Define Expected Use Cases:**

1. How will the product be used?
2. Where geographically will the product be used?
3. What physical environments will the product be used in?
4. What digital environments will the product be used in?
5. How long is the product expected to be used for?
6. What IoT product components besides the IoT device will the product rely on to function?
7. What external dependencies on other systems will the product likely have?
8. How might attackers misuse and compromise the 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?
10. What other aspects of product use might be relevant to the product’s cybersecurity risks?

# What’s Changed?

- The assertion of examining expected customers for their needs and goals in expected use cases
- The emphasis on customers purchasing products rather than simply devices
- The additional questions manufacturers can answer to anticipate how products will be deployed and used include:
  - New: 4. What digital environments will the product be used in? (e.g., unmanaged Wi-Fi networks; managed enterprise or industrial networks)
  - New: 6. What IoT product components besides the IoT device will the product rely on to function? (e.g., a backend; companion application; or specialty networking/gateway hardware)
  - Enhanced 7: with external dependencies with clarity on -- integration with third-party management applications
  - Enhanced 8: with the addition of expected physical and digital environments for -- How attackers might misuse and compromise the product
  - New: 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

# Discussion Questions for Activity 1

- What more information is needed to accurately identify expected customers for an IoT product?
- What strategies can be used to ensure the cybersecurity needs of additional users are addressed?
- How can manufacturers better define expected use cases based on anticipated customers?
- What methods can be used to validate these use cases during product development?
- How can manufacturers effectively communicate risk-related assumptions to customers?

# Activity 2: Research Customer Cybersecurity Needs and Goals

**Cybersecurity Needs and Goals of Customers:**

- Customers' cybersecurity needs are driven by unique risks and can vary significantly.
- Manufacturers can design devices to be minimally securable, addressing common cybersecurity risks and supporting customer needs.

**Cybersecurity Connections Between Manufacturers and Customers**

- Customers expect IoT devices to be secure and aligned with their cybersecurity needs, which may include using existing mechanisms and meeting regulatory requirements.
- Cybersecurity risks for IoT devices involve safeguarding both the device's functionality and the confidentiality, integrity, and availability of data.
- Manufacturers can anticipate customer cybersecurity goals based on existing guidance and requirements, ensuring their products are easier to secure.

**Utilizing Existing Guidance and Regulations:**

- Manufacturers could leverage laws, regulations, and voluntary guidance to shape their products' cybersecurity features.
- Sector-specific requirements, such as those from the FDA and HIPAA, influence cybersecurity needs and could be considered in product design**.**

# Activity 2: Research Customer Cybersecurity Needs and Goals

1. How will the IoT product interact with the physical world?
2. How will the IoT product need to be accessed, managed, and monitored by authorized people, processes, and other devices?
3. What are the known cybersecurity requirements for the IoT product?
4. How might the IoT product's use of device cybersecurity capabilities be interfered with by the device's operational or environmental characteristics?
5. What will the nature of the IoT product's data be?
6. What is the degree of trust in the IoT product that customers may need?
7. What complexities will be introduced by the IoT product interacting with other devices, systems, and environments?

# What’s Changed?

- The emphasis on customers purchasing products rather than simply devices
- Clarity added
  - Added: “Conversely, most backends store significant data related to IoT products, but some merely pass data to other IoT product components. Understanding the nature of expected data on all IoT product components”
  - Added emphasis on 'implementations’ of the cybersecurity capabilities' to emphasize
  - A paragraph inserted after the 7th question: “to clarify that by answering these questions, manufacturers can identify for each of the anticipated use cases the reasonable threats to the IoT product, how it may be vulnerable and what the resulting risks could be to customers and the operational environment. A complete assessment may not be able to be performed but an initial assessment of risk for the expected use cases will guide the identification of product cybersecurity capabilities.”
- Additional references were added for NIST SP 800-213/A for the federal profile

# Discussion Questions for Activity 2

- What information do we need to better understand customers' unique cybersecurity needs and risks?
- How would we describe a risk “action” for manufacturers as different from a risk assessment?
- How can we enhance communication about the IoT product’s cybersecurity features and limitations?
- How will the IoT product interact with other devices, systems, and environments?
- How can manufacturers leverage laws, regulations, and guidance to shape their products' cybersecurity features?

# Lunch Break

Return for 1:00pm

# Leveraging FIDO Alliance cybersecurity standards in support of IR8259

Brad Goodman

Dell

# NIST IR 8259 Revision 1 Preliminary Update:  Session 2

Mike Fagan

Technical Lead, Cybersecurity for IoT Program

# Activity 3: Determine How to Address Customer Needs and Goals

- Manufacturers can use their research on the needs and goals of IoT product’s expected customers and use cases to help customers mitigate cybersecurity risk.
- Use research to develop means of implementing cybersecurity  need and goals.
- There is need not be a one-to-one mapping for means to goals, since some goals may be met with many means and vice versa
- Not all needs and goals can or need to be addressed using only technical means, and some technical means themselves may require additional non-technical means for initial and on-going securability

# Activity 3: Determine How to Address Customer Needs and Goals

For each cybersecurity need or goal, the manufacturer can answer this question: which one or more of the following is a suitable means (or combination of means) to achieve the need or goal?

- The IoT device can provide the technical means through its device cybersecurity capabilities
- Another IoT product component related to the IoT device can provide the technical means on behalf of the IoT device
- Non-technical means can also be provided by manufacturers or other organizations (i.e., supporting entities) and services acting on behalf of the manufacturer
- The customer can select and implement other technical and non-technical means for mitigating cybersecurity risks.

# Activity 3: Determine How to Address Customer Needs and Goals

In addition to identifying suitable means for addressing each cybersecurity need and goal, manufacturers can answer **how robustly must each technical means be implemented in order to achieve each cybersecurity need or goal?**

- Does it need to be implemented in hardware and/or software?
- Which data needs to be protected, what types of protection each instance of data needs, and how strong does that protection need to be?
- How strongly an entity’s identity needs to be authenticated before granting access if the entity is a human?
- Does data received by or inputted into the device need to be validated ?
- How readily can software updates can be reverted if a problem occurs?

# What’s Changed?

- The emphasis on customers purchasing products rather than simply devices
- Removed excessive wording across sections that implied product components descriptions with additional explanation because they are now central to the overall document and clarified in up front sections of the document
- Added references to NISTIR 8259B, NISTIR 8425, and NIST SP 800-213/A

# Discussion Questions for Activity 3

- How can starting with risk related assumptions help to identify necessary cybersecurity capabilities for securing IoT products?
- How can risk related assumptions and threat modeling be used to identify cybersecurity capabilities for when the IoT product is not being used as it was designed/intended?
- What processes are the most fruitful for identifying necessary cybersecurity capabilities as early as possible in the design process?
- What common cybersecurity needs and goals have specific hardware/software implementations that need to be built into IoT products early in the design process?
- What are common challenges to developing means of meeting cybersecurity needs and goals once they've been identified?

# Discussion Questions for Activity 3

- How do IoT product baselines and similar documents help manufacturers in the process of identifying needs and goals and developing means of implementing and achieving them?
- How do manufacturers use NIST documents (8259 series, NISTIR 8425, NIST SP 800-213) alongside guidance for particular industry sectors and customer groups to help address cybersecurity needs and goals of customers?
- Where do product baseline documents like the 8259 series help to facilitate this process of identifying and meeting customer needs and goals for cybersecurity and where do they potentially create challenges for IoT product manufacturers?
- What challenges arise from trying to use product baseline documents and more specific industry standards that potentially have different audiences in mind?

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

Manufacturers can make their IoT products more securable by appropriately provisioning the device hardware & software resources

- What potential future use needs to be considered, considering lifespan and terms of support?
- Should an established IoT platform be used instead of acquiring and integrating individual hardware and software components?
- Should any of the device cybersecurity capabilities be hardware-based?
- Does the hardware or software (including the operating system) include unneeded device capabilities with cybersecurity implications? If so, can they be disabled to prevent misuse and exploitation?

Manufacturers can improve securability of IoT products by appropriately implementing product cybersecurity capabilities across all IoT product components

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

Manufacturers should consider which secure development practices  and other non-technical supporting capabilities are most appropriate to support customer needs and goals

- How is the code protected from unauthorized access and tampering?
- How can customers verify hardware or software integrity for the IoT device or other IoT product components?
- What verification is done to confirm that the security of third-party software used within the IoT product meets the customers’ needs?
- What measures are taken to minimize the vulnerabilities in released IoT product software?
- What measures are taken to accept reports of possible IoT product software vulnerabilities and respond to them? And to assess and prioritize the remediation of vulnerabilities in IoT product software?

# What’s Changed?

- The emphasis on customers purchasing products rather than simply devices
- Enhanced “1. Considering expected terms of support and lifespan, what potential future use needs to be taken into account?” with the additional statement: "The ability for customers to determine the support status for products is important to making products securable."
- Added paragraph: "Beyond the IoT device, manufacturers can improve securability of IoT products by appropriately implementing product cybersecurity capabilities across all IoT product components. For example, data stored in backends, companion applications, or specialty networking/gateway hardware should be protected using the same or similar means to protect data as in the IoT device. When designing or selecting hardware and software resources for IoT product components other than IoT devices, manufacturers can answer the following questions for the expected customers and use cases to help identify provisioning needs and potential issues."
  - We plan to add questions under this as with other portions of this activity
- Added emphasis on 'other non-technical supporting capabilities' language.

# Discussion Questions for Activity 4

- Are there additional considerations that should be included for manufacturers in appropriately provisioning computing resources (i.e., hardware and software)?
- **What questions should be included for manufacturers to consider when planning for cybersecurity capabilities across all IoT product components?**
- Are there additional considerations that should be included for manufacturers in determining appropriate secure development practices and other non-technical supporting capabilities?
- Are there additional considerations for manufacturers in planning adequate support for customer needs and goals (other than provisioning computing resources and planning non-technical supporting capabilities)?

# 15 Minute Break

# NIST IR 8259 Revision 1 Preliminary Update:  Session 3

Mike Fagan

Technical Lead, Cybersecurity for IoT Program

# Activity 5: Define Approaches for Communicating with Customers: Questions

- Communication with the customer has to be customer-centric in terms and through means tailored to the expected customers
  - Terminology
  - Location
  - Level of detail
- Manufacturer is responsible for establishing an overall communication plan for the product that can manage any needed communication between suppliers and customer about product components.

# Activity 5: Define Approaches for Communicating with Customers: Questions

1. What is the purpose of the communication? (New)
2. What terminology will the customer understand?
3. How much information will the customer need?
4. How/where will the information be provided?
5. How will the integrity of the information be verified?
6. How will customers communicate with you as the manufacturer?

# What's Changed?

- Added 1. "What is the purpose of the communication? Communicating cybersecurity information incurs a cost, monetary and otherwise for both the manufacturer and customer. The manufacturer must prepare and effectively deliver the message while customers must expend time and effort to understand and decide how to use the information. As such, cybersecurity communications should be focused on key disclosures or calls for action to customers."

# Discussion Questions for Activity 5

- Is there additional guidance around communication approaches needed?
- What more should be considered in discussing communication channels  back to manufacturer?
  - Cybersecurity questions
  - Vulnerability or anomaly reports
- What about unexpected customers for an IoT product?
  - Consumer IoT used in business setting
  - Small business unfamiliar with terminology

# Activity 6: Decide What to Communicate to Customers and How to Communicate it: 6 areas

- Cybersecurity Risk-Related Assumptions
- Support and Lifespan Expectations
- Device Composition and Capabilities
- Software Updates
- Product Retirement Options
- Technical and Non-Technical Cybersecurity Capabilities

# What’s Changed?

- An emphasis on customers purchasing products rather than simply devices.
- Under 4.2.2. Support and Lifespan Expectations
    - Enhanced “3. What functionality, if any, will the product have after support ends and at end-of-life?” with the additional emphasis: "(i.e., will a freezer continue to function as a freezer even if automatic inventorying applications are not available)"
    - Enhanced “4. How can customers report suspected problems with cybersecurity implications, such as software vulnerabilities, to the manufacturer? Will reports be accepted after support ends? Will reports be accepted after end-of-life?” with the additional emphasis on: "Will any action be taken with these reports (e.g., posting to a website) after support ends?"

# What’s Changed?

- Under 4.2.4 Software Updates
  - Added: "This may vary for different IoT product components. For example, IoT devices may be managed by customers in many cases, but most backends will not“ under: “4.Which entity (e.g., customer, manufacturer, third party) is responsible for performing updates? Or can the customer designate which entity will be responsible (e.g., automatically applied by the manufacturer)?”
- Under 4.2.6 Technical and Non-Technical 'Means' was adjusted to 'Cybersecurity Capabilities' throughout.
- Removed excessive wording in the first paragraph that emphasized technical means to clarify cybersecurity capabilities.

# Discussion Questions for Activity 6

- When, where and how should assumptions and expectations for use be brought to the customer’s attention?
- If the customer is violating assumptions and expectations, how should this be flagged to the customer?
- Trend is toward greater manufacturer responsibility, should that have greater emphasis?
- Should there be greater transparency encouraged in communicating about what data is collected, how it is stored, options for deletion, and data access by third parties?

# Discussion Questions for Activity 6

- How do we balance transparency for customers with ability of manufacturers to commit to length of support?
- What notification should be expected to customers about a change in the planned end of support?
- What does support for repairability mean for cybersecurity especially post-end of support?
- How viable is open-source community maintenance of IoT software post-end of support?

# Discussion Questions for Activity 6

- Customers need information about data cleansing when ready to retire or reprovision the product
  - How can customers get information when needed (potentially years after purchase)?
  - How should manufacturers treat products that are more likely to change ownership? (e.g., large appliances, industrial equipment, vehicles)
- How can product manufacturers maintain product information?
- How can manufacturers act as a central point of contact for questions and info on all components of the IoT product?

# Closing Remarks

Mike Fagan

Program Manager, Cybersecurity for IoT Program

# THANK YOU

## CONTACT US

NIST.gov/cybersecurity

@NISTcyber

NIST Cybersecurity for
IoT Program Home Page