National Institute of Standards and Technology
U.S. Department of Commerce

Rounding Up Your IoT Security Requirements:

Draft NIST Guidance for Federal Agencies

Katerina Megas

Program Manager,

NIST Cybersecurity for IoT Program

Agenda

- Background on the NIST ITL, and the Cybersecurity for IoT Program
- Introduce the four public drafts released in December:

NISTIR 8259B, *IoT Non-Technical Supporting Capability Core Baseline*

NISTIR 8259C, *Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline*

NISTIR 8259D, *Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government*

SP 800-213, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*

- Solicit Community Feedback & Describe Next Steps

The NIST Information Technology Lab's purpose is to cultivate trust in IT and metrology.

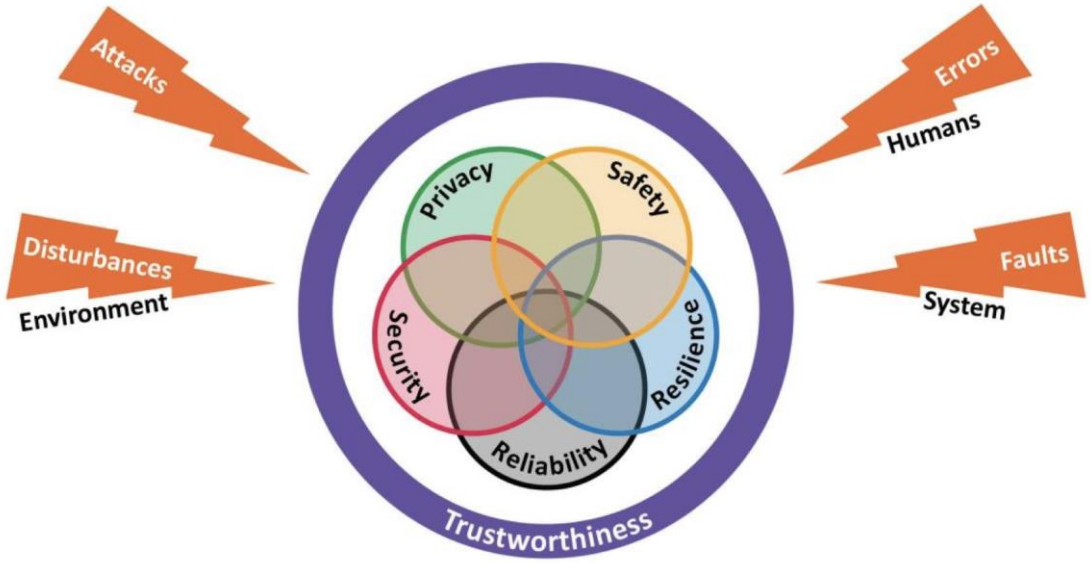
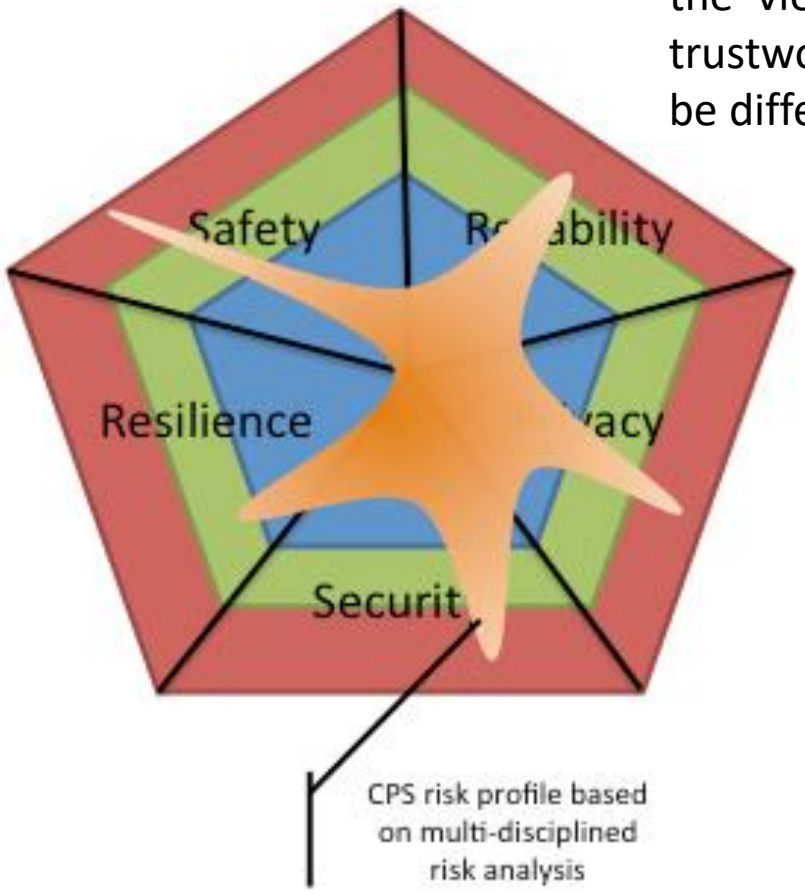


Figure 1: IoT Trustworthiness - IIC Industrial Internet Security Framework - source IIC IISF

Organizations need to consider all 5 aspects of Trustworthiness: Safety, Security, Privacy, Resilience and Reliability

Depending on the risk the 'view' of the trustworthiness will be different



Core Principles Guiding Our Efforts

Cybersecurity for IoT Program Principles

Risk-Based Understanding

IoT capabilities, behaviors, deployment environments, and other characteristics can affect cybersecurity risk. Our approach to managing this risk is rooted in an understanding of how IoT can affect it.

No One Size Fits All

Each organization has its own risk tolerance and mission needs, and no one set of controls will address the wide range of cross-industry and cross-vertical needs and use cases. There is no one-size-fits-all approach to managing IoT cybersecurity risk.

Ecosystem of Things

Recognizing that no device exists in a vacuum, NIST takes an ecosystem approach to IoT cybersecurity. For many devices, much of the functionality happens outside the device—not all the security is on the device itself. As such, we look at the entire ecosystem, not just endpoints.

Outcome-Based Approach

Embrace the Cybersecurity Framework's outcome-based approach. Specify desired cybersecurity outcomes, not necessarily how to achieve those outcomes, which allows organizations to choose the best solution for each IoT device and/or their enterprise environment.

Stakeholder Engagement

NIST works with diverse stakeholders to advance IoT cybersecurity. This includes collaborating with stakeholders to provide the necessary tools, guidance, standards, and resources.

A little background on NIST and the IoT Cybersecurity Program

- Non-Regulatory agency and technical arm of the U.S. Department of Commerce
- NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
- In accordance with the Federal Information Security Modernization Act (FISMA), NIST develops information security standards and guidelines for federal information systems.

IoT cybersecurity related initiatives

Research/Reports

- Mitigating IoT-Based DDoS/Botnet Report
- Cybersecurity for Cyber Physical Systems
- Cybersecurity Framework
- Cybersecurity Framework Manufacturing Profile
- Cybersecurity for Smart Grid Systems
- Cyber Threat Information Sharing
- Lightweight Encryption
- Low Power Wide Area IoT
- Network of Things
- Report on State of International Cybersecurity Standards for IoT
- Security and privacy concerns of intelligent virtual assistances
- Security of Interactive and Automated Access Management Using Secure Shell (SSH)
- Considerations for Managing IoT Cybersecurity and Privacy Risks
- Core Cybersecurity Feature Baseline for Securable IoT Devices
- Trustworthy Network of Things

Special Publications

- BLE Bluetooth
- Cloud security
- Digital Identity Guidelines
- Guide to Industrial Control Systems (ICS) Security
- RFID Security Guidelines
- Software Assessment Management Standards and Guidelines
- Supply Chain Risk Management
- Security Content Automation Protocol (SCAP) Standards and Guidelines
- Security Systems Engineering
- ABCs of Conformity Assessment
- Conformity Assessment Considerations for Federal Agencies

Applied

- Galois IoT Authentication & PDS Pilot
- GSMA Trusted Identities Pilot
- National Vulnerability Database
- Securing the Industrial IoT (IIoT)
- IIoT-Based Automated Distributed Threats
- Capabilities Assessment for Securing Manufacturing Industrial Control Systems
- Security Review of Consumer Home IoT Products
- Security for IoT Sensor Networks
- Healthcare Sector Projects
  - Wireless Infusion Pumps
  - Securing Telehealth Remote Patient Monitoring Ecosystem
- Privacy Engineering Program
- Zero Trust Architecture Project
- IoT Device Network-Layer Onboarding Taxonomy

National Institute of Standards and Technology
U.S. Department of Commerce

Key Events In the IoT Cybersecurity Program

NISTIR 8201 (Dec 2017)

- NIST IR 8200 – Status of International IoT Cybersecurity Standardization
- Takeaways from Oct 2017 Colloquium
  - IoT did introduce new risks and challenges
    - No one size fits all
    - Would require an ecosystem approach
    - Risk based understanding
    - Outcome based
  - Lots of existing guidance applicable
  - Focus on the gaps
  - Provide guidance to help tie together all the guidance

NISTIR 8228 (June 2019)

- Focuses on what is different about managing risks associated with the use of IoT
- Frames IoT risks and challenges in the context of implementation of SP800-53 controls and Cybersecurity Framework
- *Customers dependent on security capabilities of IoT devices*

NISTIR 8259 / 8259A (May 2020)

- Three public workshops, two public comment periods and over 600 comments
- Cybersecurity recommendations for IoT device manufacturers
- Activities for manufacturers to incorporate into product development lifecycle
- Six core Cybersecurity capabilities for IoT devices

Federal Profile Workshop (Jul 2020)

- Published on GitHub analysis of SP 800-53 controls dependencies on IoT device capabilities. Suggested this to be a 'catalogue' for agency use
- Takeaways
  - Confirmed device centric approach useful
  - Confirmed that non-technical dependencies need to be identified
  - Confidence mechanisms desired for the market but more discussions required

4 Public Drafts (Dec 2020)

- Non-Technical Supporting Activities Baseline recommended for all IoT device manufacturers
- NIST published the process NIST followed to adapt the baseline to Federal agency use case
- Starting point for agencies in a Federal profile identifying the key capabilities likely needed to support agency implementation of Low baseline
- Guidance for Federal Agencies with considerations for IoT risk in agency RMF processes and how to develop requirements for IoT devices leveraging catalogue and Federal profile

Botnet Report (May 2018)

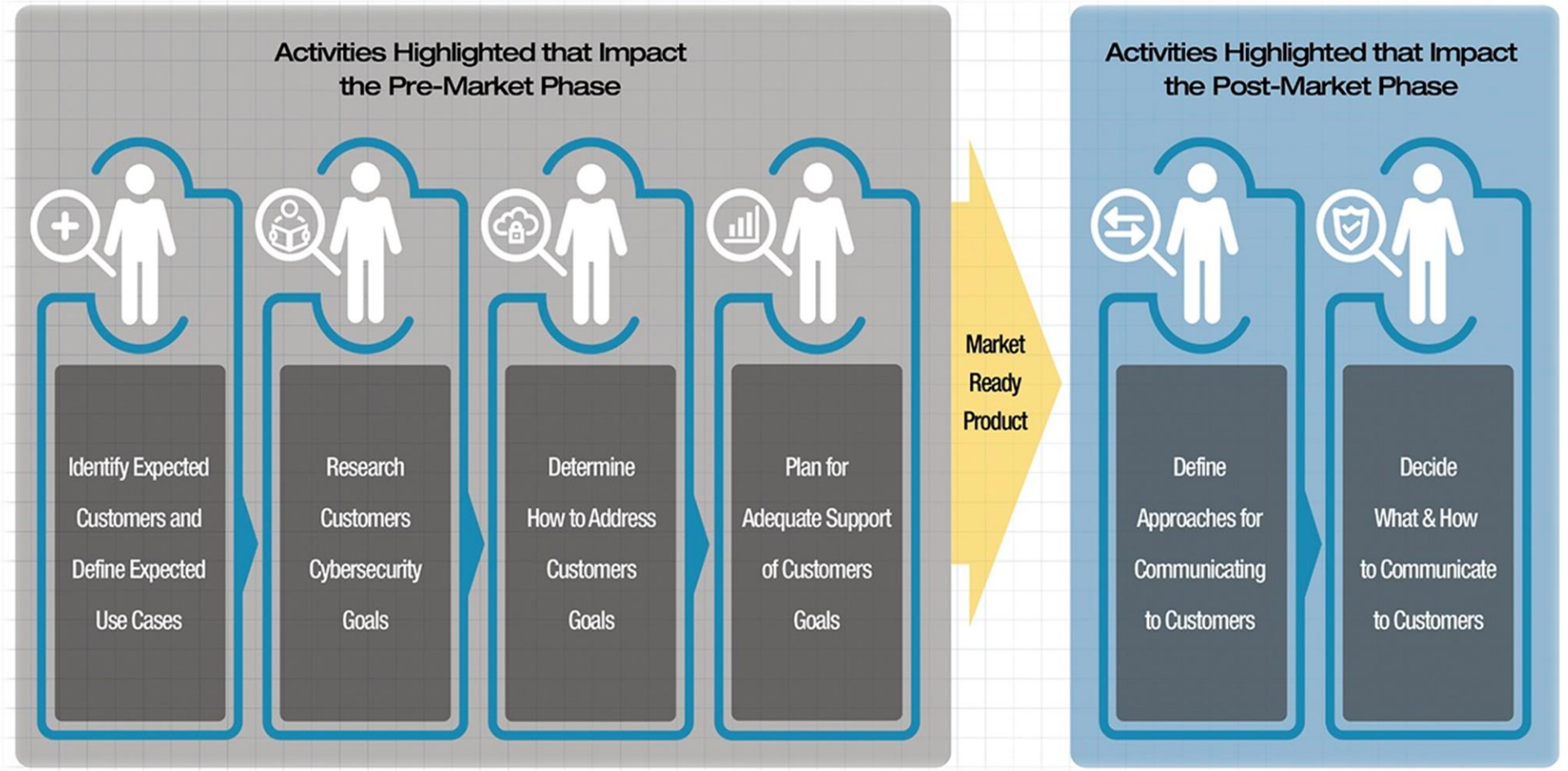
Botnet Roadmap (Nov 2018)

Botnet Report Update (July 2020)

IoT Cybersecurity Improvement Act (Dec 2020)

Released NISTIR 8259 (May 2020)

Recommended activities to help manufacturers address customer needs for IoT cybersecurity in their product development processes



Wait: Now We Have *Two* Baselines?

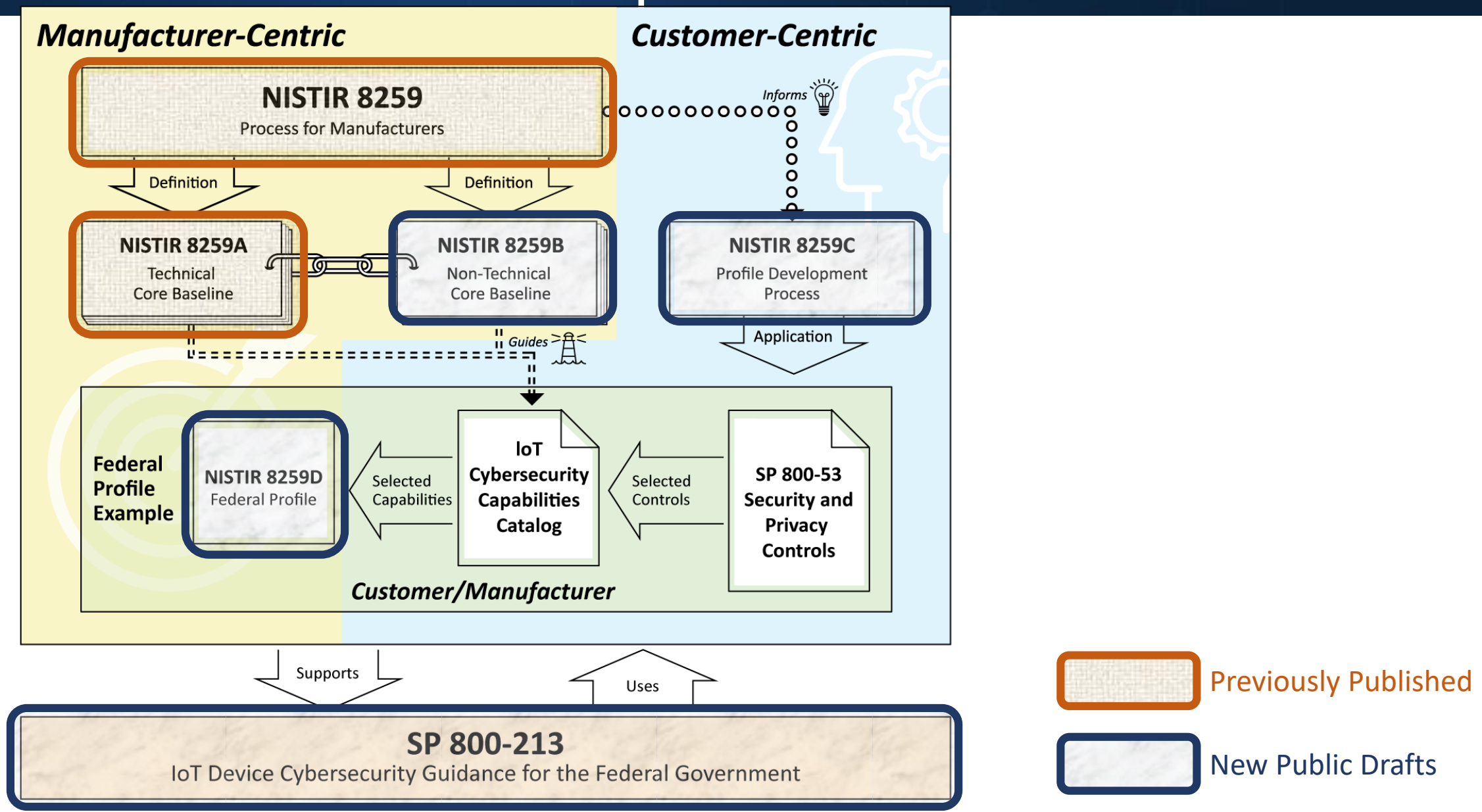
NISTIR 8259A (May 2020) Technical Baseline

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

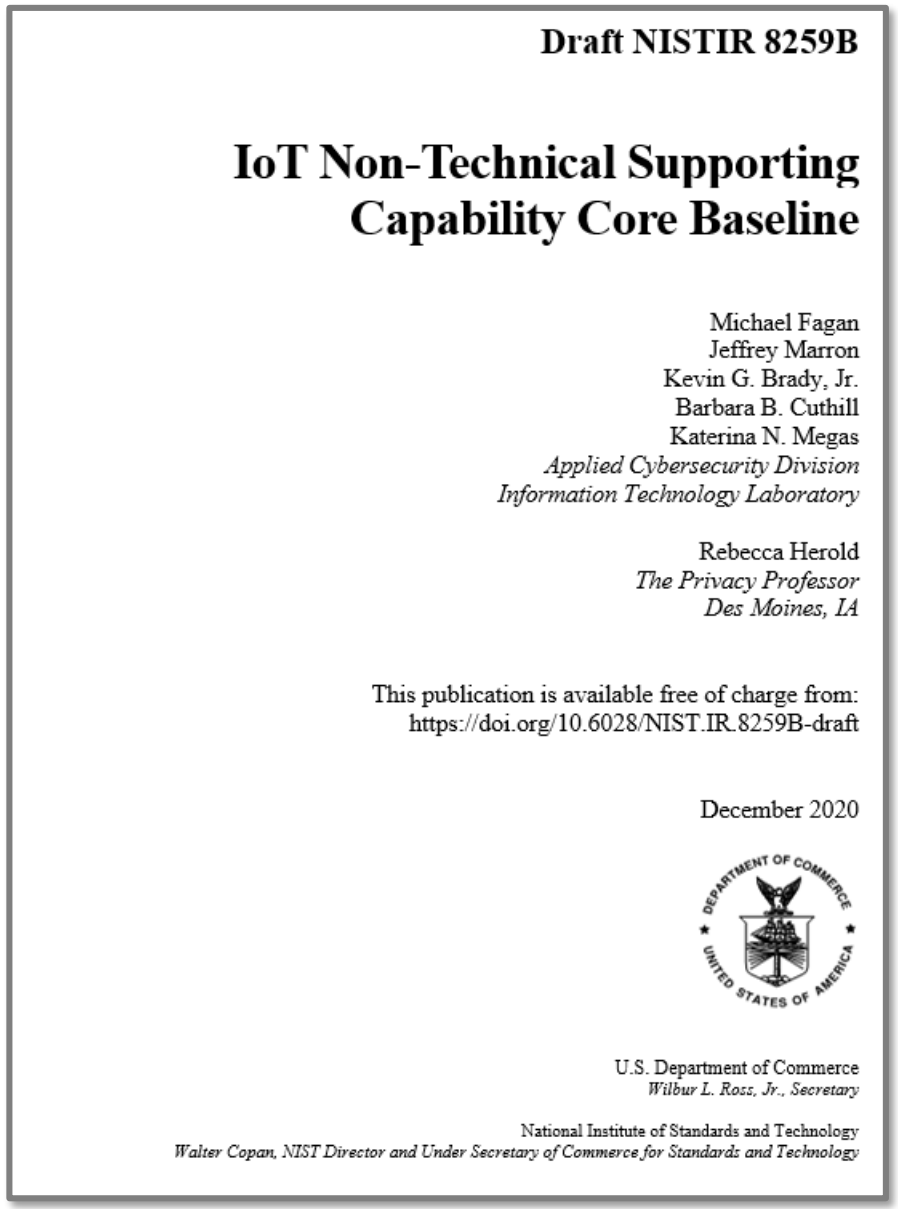
Draft NISTIR 8259B (Dec 2020) Non-Technical Baseline

- Documentation
- Information & Query Reception
- Information Dissemination
- Education & Awareness

Assembling The Pieces: Four New Publications Expand Our Guidance



Next Up …



Draft NISTIR 8259B

IoT Non-Technical Supporting Capability Core Baseline

Michael Fagan
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
Katerina N. Megas
Applied Cybersecurity Division
Information Technology Laboratory

Rebecca Herold
The Privacy Professor
Des Moines, IA

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8259B-draft

December 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

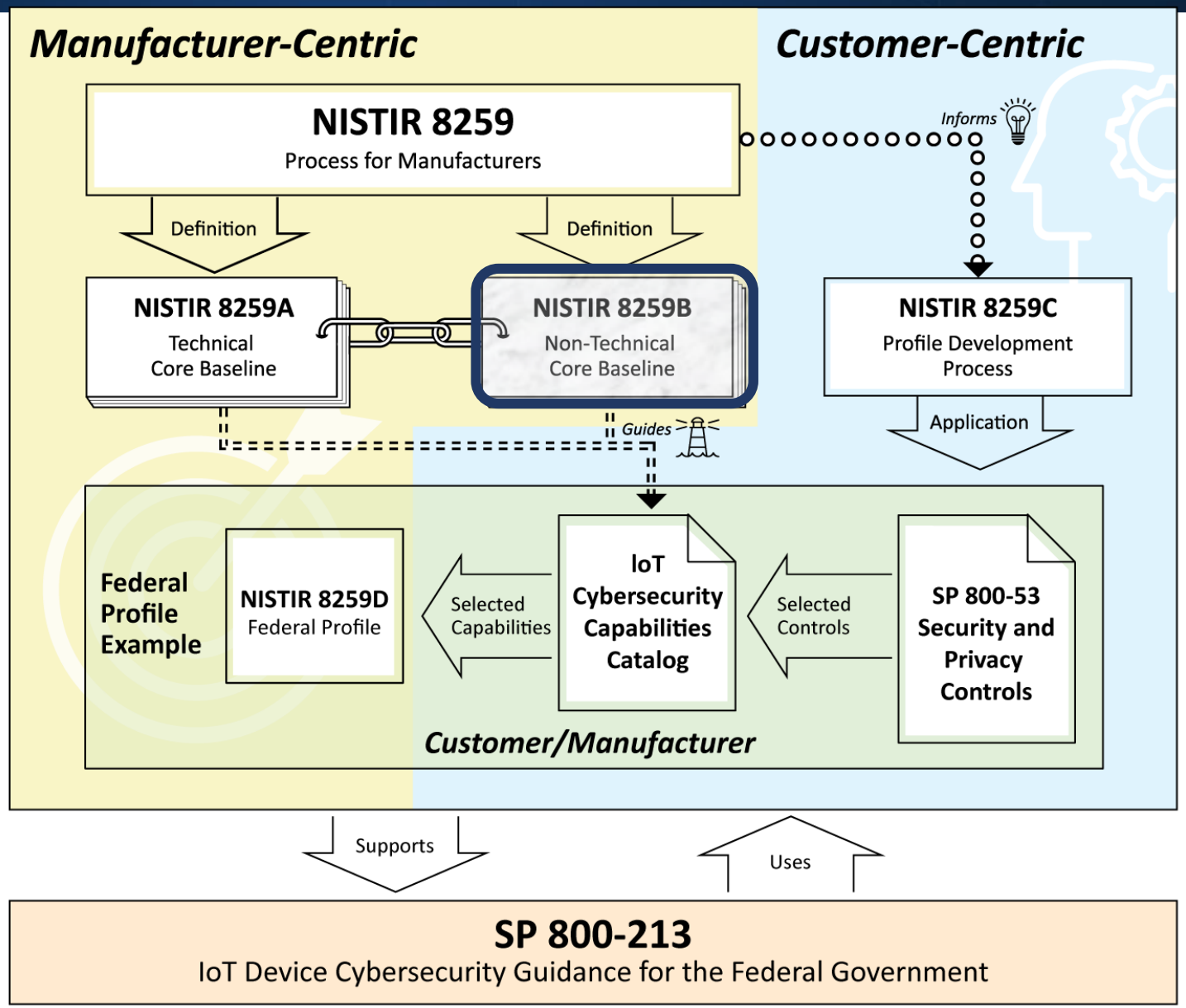
NISTIR 8259B, *IoT Non-Technical Supporting Capability Core Baseline*

Presenter:
Rebecca Herold

National Institute of Standards and Technology
U.S. Department of Commerce

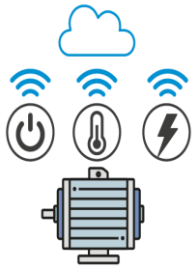
Draft NISTIR 8259B: IoT Non-Technical Supporting Capability Core Baseline

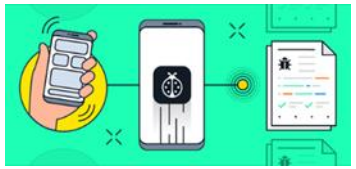
8259B in Context



What is Meant by Non-Technical Capabilities?

- Policies and procedures
- Training and awareness
- Providing support to tech users
- Changing settings on tech devices
- Risk management activities
- Disposal practices
- Physical protections
- Vulnerability assessments
- Bug reporting
- Contracts
- Audits
- Contingency plans
- Systems and applications development lifecycles
- Compliance





Images Show a Few Examples of Unlimited Possibilities

Purpose of the 8259B Guidance

Defines the non-technical supporting capabilities used to support common cybersecurity technical controls.

Documentation

Information and Query Reception

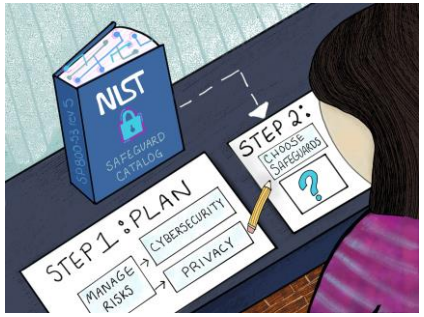
Information Dissemination

Education and Awareness

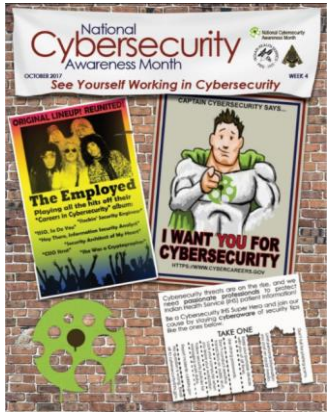
“Documentation” Capability

Definition:
The ability for the manufacturer and/or supporting entity to create, gather, and store information relevant to cybersecurity of the IoT device throughout the development of a device and its subsequent lifecycle.

Sub-Capabilities:
1. Document assumptions made during the development process and other expectations related to the IoT device.
2. Document the device cybersecurity capabilities, such as those detailed within NISTIR 8259A, that are implemented within the IoT device and how to configure and use them.
3. Document device design and support considerations related to the IoT device.
4. Document maintenance requirements for the device.



Credit: N. Hanacek/NIST

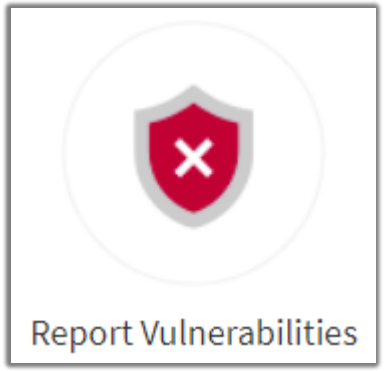


Many examples of specific non-technical actions for the corresponding sub-capability are provided

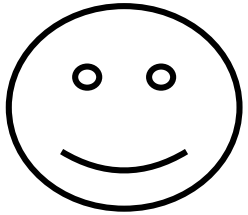
“Information and Query Reception” Capability

Definition:
The ability for the manufacturer and/or supporting entity to receive from the customer information and queries related to cybersecurity of the IoT device.

Sub-Capabilities:
1. The ability for the manufacturer and/or supporting entity to receive maintenance and vulnerability information (e.g., bug reporting capabilities, bug bounty programs) from their customers and other types of entities
2. The ability for the manufacturer and/or supporting entity to respond to customer and third-party queries about cybersecurity of the IoT device (e.g., customer support)



Source: https://us-cert.cisa.gov/report


Manufacturer/ Vendor

“I’d like to request a user security control feature for you to build into the IoT device you manufacture…”

IoT Customer

“I’ve found a possible security vulnerability in your IoT device. When I…”

IoT Customer

Many examples of specific non-technical actions for the corresponding sub-capability are provided

“Information Dissemination” Capability

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

Sub-Capabilities:

1. The procedures to support the ability for the manufacturer and/or supporting entity to alert customers of the IoT device about cybersecurity relevant information.
2. The procedures to support informing customers of activities and procedures used by the manufacturer and/or supporting entity to further consider and safeguard the cybersecurity of the device.
3. The procedures to support the ability for the manufacturer and/or supporting entity to notify customers of cybersecurity-related events and information related to an IoT device throughout the support lifecycle.

Many examples of specific non-technical actions for the corresponding sub-capability are provided

“Education and Awareness” Capability

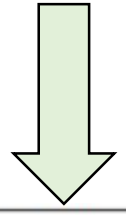
Definition:
The ability for the manufacturer and/or supporting entity to create awareness of and educate customers about cybersecurity-related information, considerations, features, etc. of the IoT device.

Many examples of specific non-technical actions for the corresponding sub-capability are provided

Sub-Capabilities:

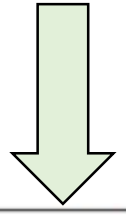
1. Educate customers of the IoT device about the presence and use of device cybersecurity capabilities.
2. Educate customers about how an IoT device can be securely reprovisioned or disposed of.
3. Make customers aware of their cybersecurity responsibilities related to the IoT device and how responsibilities may be shared between them and others, such as the IoT device manufacturer. (e.g., related to maintenance of the IoT device)
4. Make customers aware of key assumptions and expectations related to the cybersecurity of the IoT device.
5. Educate customers about how to back-up the data collected from or derived by the IoT device, and how to access such data that is stored in cloud storage, or other repositories.
6. Educate customers about vulnerability management options (e.g., anti-malware) available for the IoT device or associated system that could be used by customers.

Explain the Table To Me! (1/4)



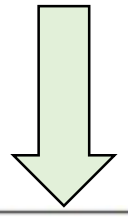
Non-Technical Supporting Capability	Common Actions	Rationale	IoT Reference Examples
Information and Query Reception: The ability for the manufacturer and/or supporting entity to receive from the customer information and queries related to cybersecurity of the IoT device.	1. The ability for the manufacturer and/or supporting entity to receive maintenance and vulnerability information (e.g., bug reporting capabilities, bug bounty programs) from their customers and other types of entities 2. The ability for the manufacturer and/or supporting entity to respond to customer and third-party queries about cybersecurity of the IoT device (e.g., customer support)	• This capability provides input for the manufacturer to in turn use in the Information Dissemination and Education and Awareness non-technical supporting capability. • Customer organizations and third-parties may want, or be required, to report vulnerabilities they identify in an IoT device. • Manufacturers can use reports of common queries and vulnerabilities to identify ways to improve the cybersecurity of the IoT device. • For broadly used IoT devices, some customers may need additional support to securely provision and use an IoT device.	•

Explain the Table To Me! (2/4)



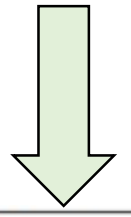
Non-Technical Supporting Capability	Common Actions	Rationale	IoT Reference Examples
Information and Query Reception: The ability for the manufacturer and/or supporting entity to receive from the customer information and queries related to cybersecurity of the IoT device.	1. The ability for the manufacturer and/or supporting entity to receive maintenance and vulnerability information (e.g., bug reporting capabilities, bug bounty programs) from their customers and other types of entities 2. The ability for the manufacturer and/or supporting entity to respond to customer and third-party queries about cybersecurity of the IoT device (e.g., customer support)	• This capability provides input for the manufacturer to in turn use in the Information Dissemination and Education and Awareness non-technical supporting capability. • Customer organizations and third-parties may want, or be required, to report vulnerabilities they identify in an IoT device. • Manufacturers can use reports of common queries and vulnerabilities to identify ways to improve the cybersecurity of the IoT device. • For broadly used IoT devices, some customers may need additional support to securely provision and use an IoT device.	•

Explain the Table To Me! (3/4)



Non-Technical Supporting Capability	Common Actions	Rationale	IoT Reference Examples
Information and Query Reception: The ability for the manufacturer and/or supporting entity to receive from the customer information and queries related to cybersecurity of the IoT device.	1. The ability for the manufacturer and/or supporting entity to receive maintenance and vulnerability information (e.g., bug reporting capabilities, bug bounty programs) from their customers and other types of entities 2. The ability for the manufacturer and/or supporting entity to respond to customer and third-party queries about cybersecurity of the IoT device (e.g., customer support)	• This capability provides input for the manufacturer to in turn use in the Information Dissemination and Education and Awareness non-technical supporting capability. • Customer organizations and third-parties may want, or be required, to report vulnerabilities they identify in an IoT device. • Manufacturers can use reports of common queries and vulnerabilities to identify ways to improve the cybersecurity of the IoT device. • For broadly used IoT devices, some customers may need additional support to securely provision and use an IoT device.	•

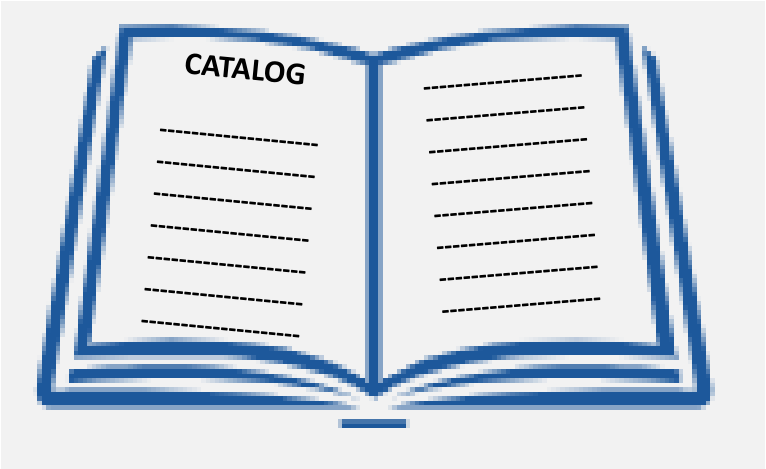
Explain the Table To Me! (4/4)



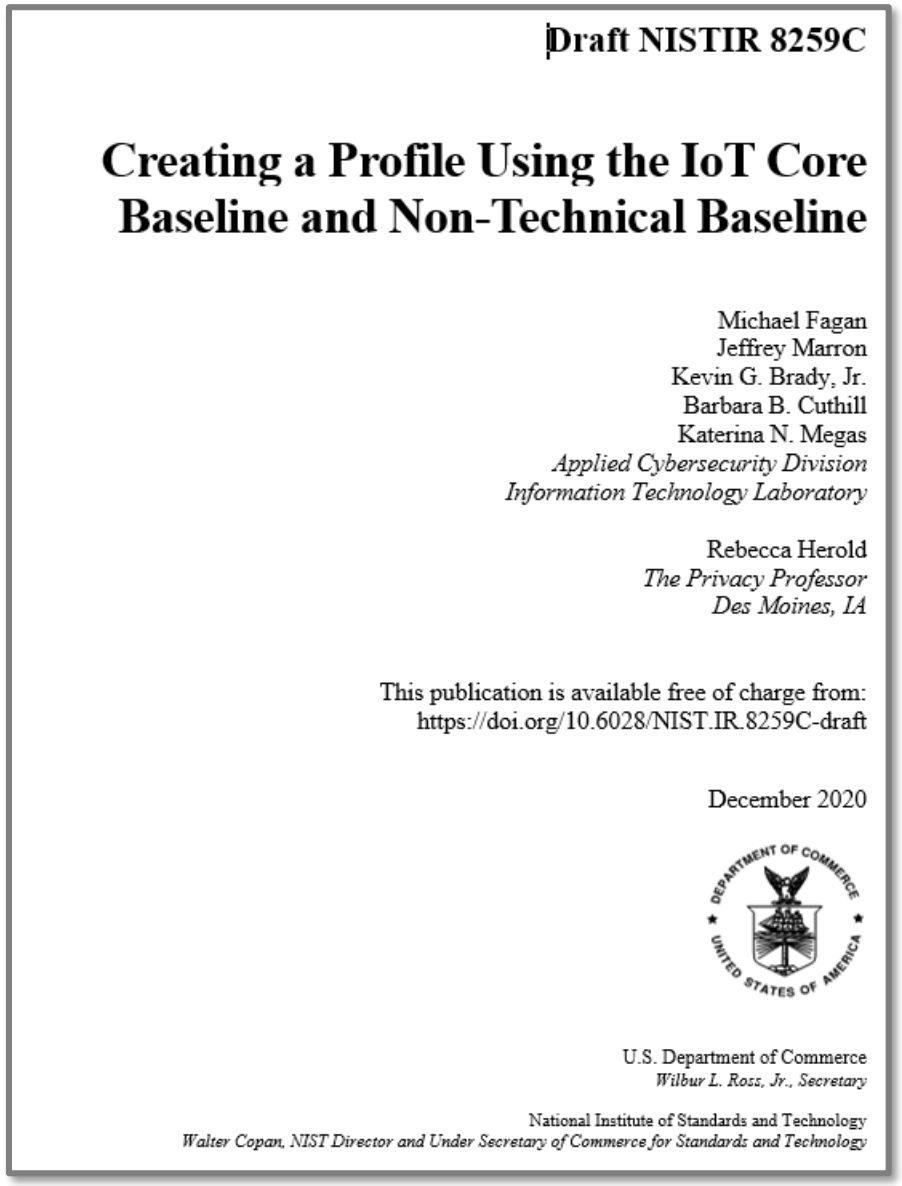
Non-Technical Supporting Capability	Common Actions	Rationale	IoT Reference Examples
Information and Query Reception: The ability for the manufacturer and/or supporting entity to receive from the customer information and queries related to cybersecurity of the IoT device.	1. The ability for the manufacturer and/or supporting entity to receive maintenance and vulnerability information (e.g., bug reporting capabilities, bug bounty programs) from their customers and other types of entities 2. The ability for the manufacturer and/or supporting entity to respond to customer and third-party queries about cybersecurity of the IoT device (e.g., customer support)	• This capability provides input for the manufacturer to in turn use in the Information Dissemination and Education and Awareness non-technical supporting capability. • Customer organizations and third-parties may want, or be required, to report vulnerabilities they identify in an IoT device. • Manufacturers can use reports of common queries and vulnerabilities to identify ways to improve the cybersecurity of the IoT device. • For broadly used IoT devices, some customers may need additional support to securely provision and use an IoT device.	•

Keep This In Mind…

- 8259B establishes the federal non-technical core baseline
- The target audiences are manufacturers, vendors, and their supporting entities
- There are many additional non-technical actions in the full NIST IoT Cybersecurity Non-Technical Capabilities Catalog



Next Up …



Draft NISTIR 8259C

Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline

Michael Fagan
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
Katerina N. Megas
Applied Cybersecurity Division
Information Technology Laboratory

Rebecca Herold
The Privacy Professor
Des Moines, IA

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8259C-draft

December 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

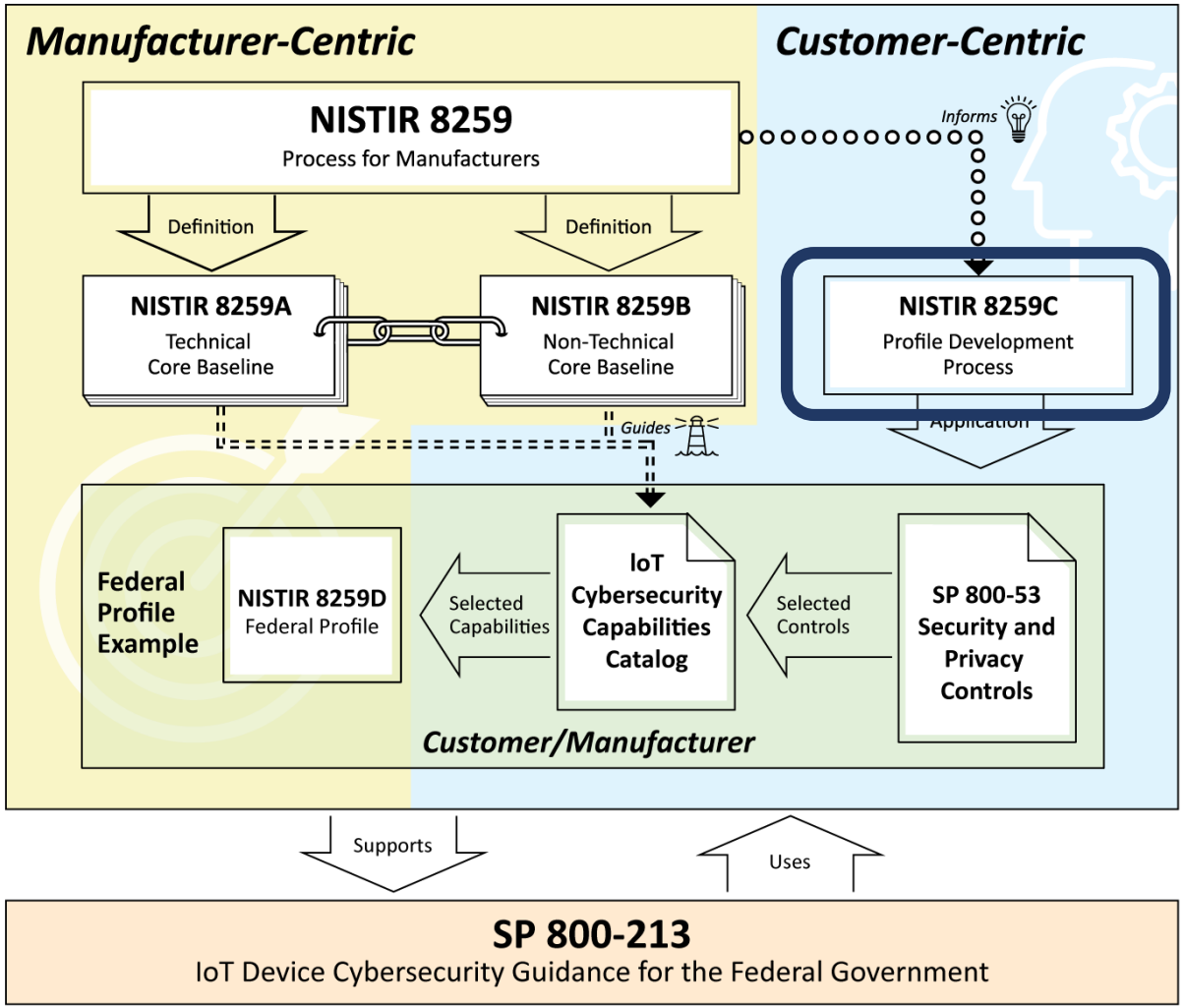
NISTIR 8259C, *Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline*

Presenter:
Kevin G. Brady, Jr.

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NISTIR 8259C: Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline

Guidance Overview

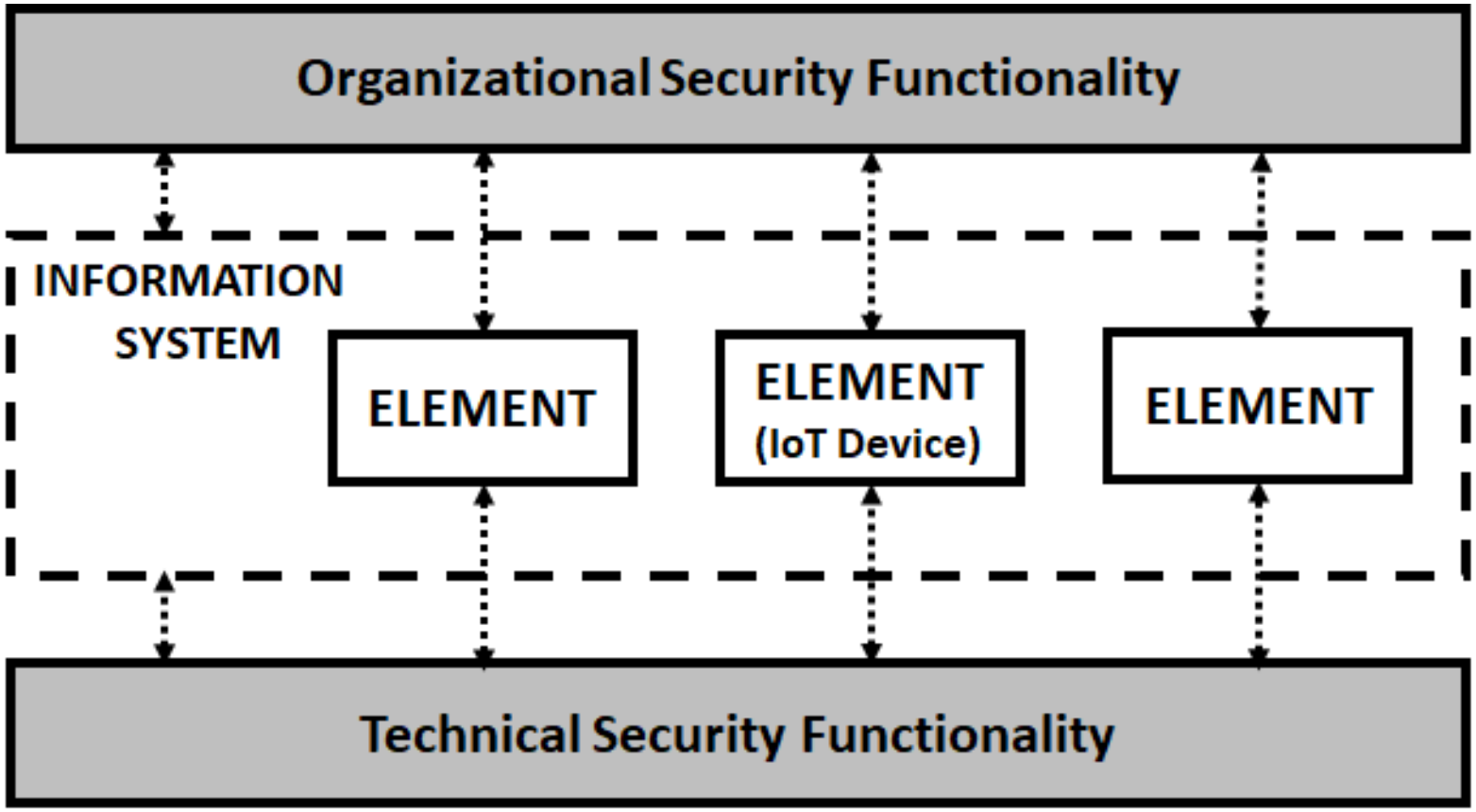


Creating Customized Profiles

- **NISTIR 8259** *Foundational Cybersecurity Activities for IoT Device Manufacturers*
  i. Activity 3 – “Determine how to address customer needs and goals”
- **NISTIR 8259 A & B**
  i. NISTIR 8259A - *IoT Device Cybersecurity Capability Core Baseline*
  ii. NISTIR 8259B - *IoT Non-Technical Supporting Capability Core Baseline*
- **Use technical and non-technical capabilities catalogs to create a customized profile of device cybersecurity capabilities and non-technical supporting actions needed to make a device securable**

Information System Overview

- **Information Systems contain ”elements” that must conform to and support technical and organizational cybersecurity capabilities**



Three Central Concepts For Creating a Profile

- **Device-Centricity**
  i. Cybersecurity guidance tends to be focused on the network, system, and organization level
  ii. Challenges for Manufacturers
    - Increasing number of IoT devices
    - Increasing complexity of cybersecurity
    - Diversity of customer use cases
    - IoT device functionality
  iii. Taking a device-centric view helps manufacturers support cybersecurity goals

Three Central Concepts For Creating a Profile

- **Cybersecurity Focus**
  i. Organizations have many competing goals:
     - Requirements for IoT device and its environment of operation
     - Demonstrating Compliance to Sector Regulations/Standards
     - Safety, Resiliency, Reliability, Privacy, and other goals depending on the use case.

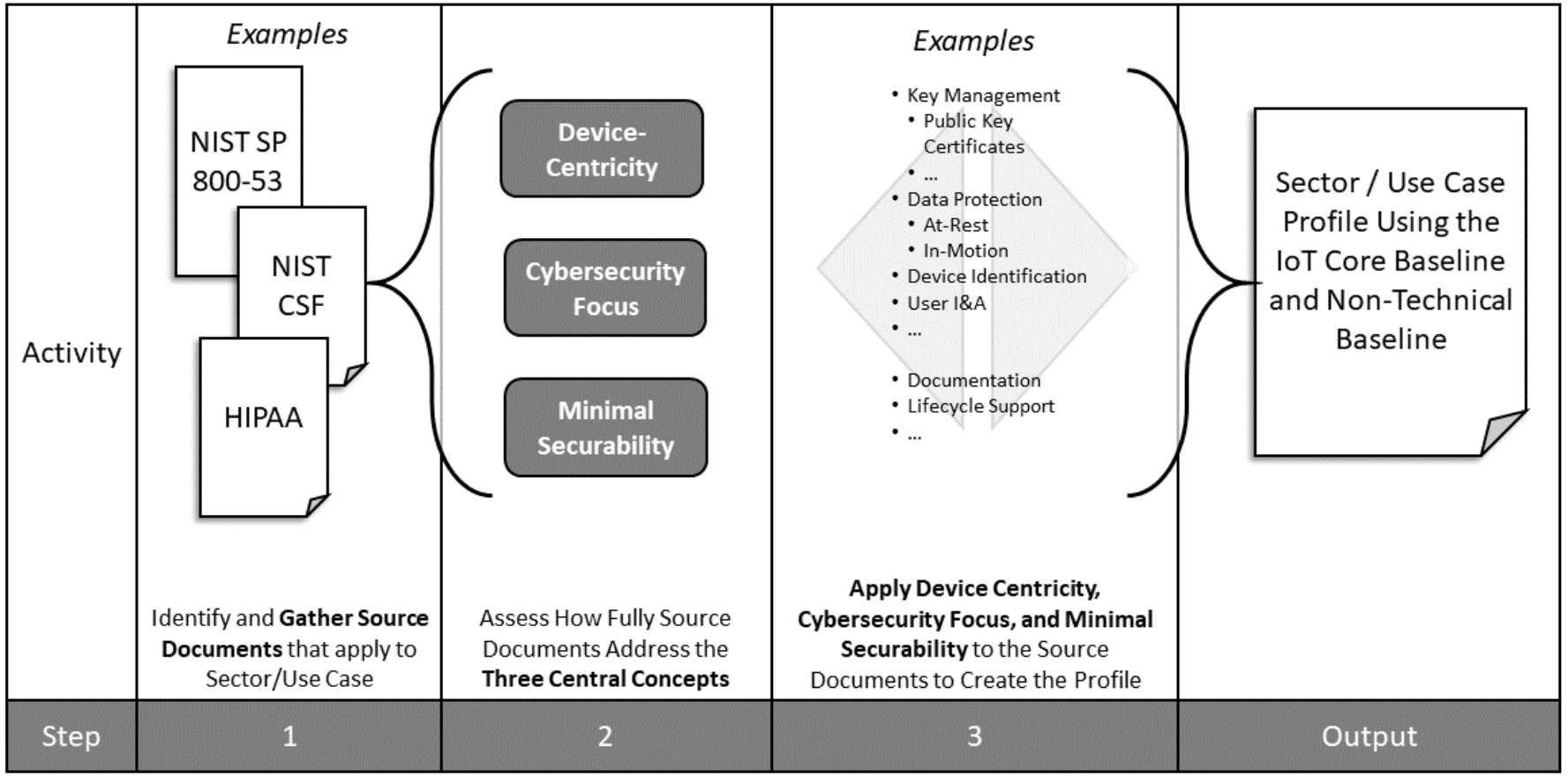
  ii. Cybersecurity needs to have its own focus in combination with other potentially conflicting goals

Three Central Concepts For Creating a Profile

- **Minimal Securability**
  i. NISTIR 8259 defines a *minimally securable* IoT device as one that has "the device cybersecurity capabilities customers may need to mitigate some common cybersecurity risks, thus helping to at least partially achieve their goals and fulfill their needs."
  ii. Manufacturer's role in IoT device cybersecurity
  iii. Other factors can influence what constitutes minimal securability

Creating a Profile

- **Steps to creating a profile using the core baseline and the non-technical baseline**



Creating a Profile

1. **Identify and Gather Source Documents for Sector/Use Case Cybersecurity Requirements**
    - Why are these documents important to the profiling process?
    - What can be used as a Source Document?
    - Source documents may vary across industry sectors and use cases

Creating a Profile

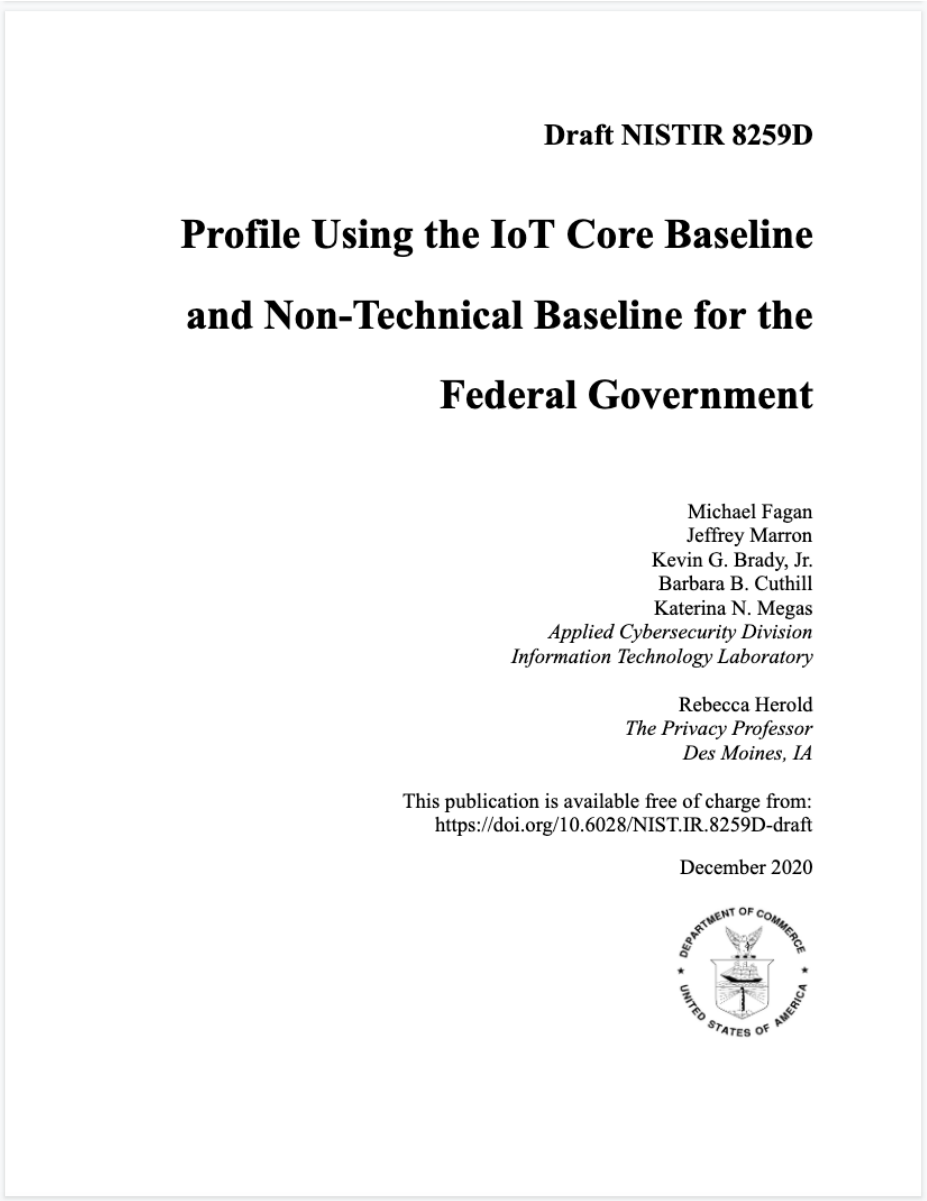
2. Assess to What Extent the Source Documents Address the Three Concepts

- Device-Centric vs Organization-Centric
- Cybersecurity focused vs non cybersecurity focused documents
- What if Source Documents do not explicitly have cybersecurity requirements?
- What if a document does not address all three concepts?

Creating a Profile

3. **Apply the Three Concepts to Source Documents to Create a Profile**
    - Analyze Source Documents Individually
    - Develop a list of device capabilities and supporting actions
    - Combine both into a coherent catalog
    - Check catalog against additional sources
    - Use minimal securability as a final filter to finalize the capabilities and actions into a profile

Next Up …



Draft NISTIR 8259D

Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government

Michael Fagan
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
Katerina N. Megas
Applied Cybersecurity Division
Information Technology Laboratory

Rebecca Herold
The Privacy Professor
Des Moines, IA

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8259D-draft

December 2020

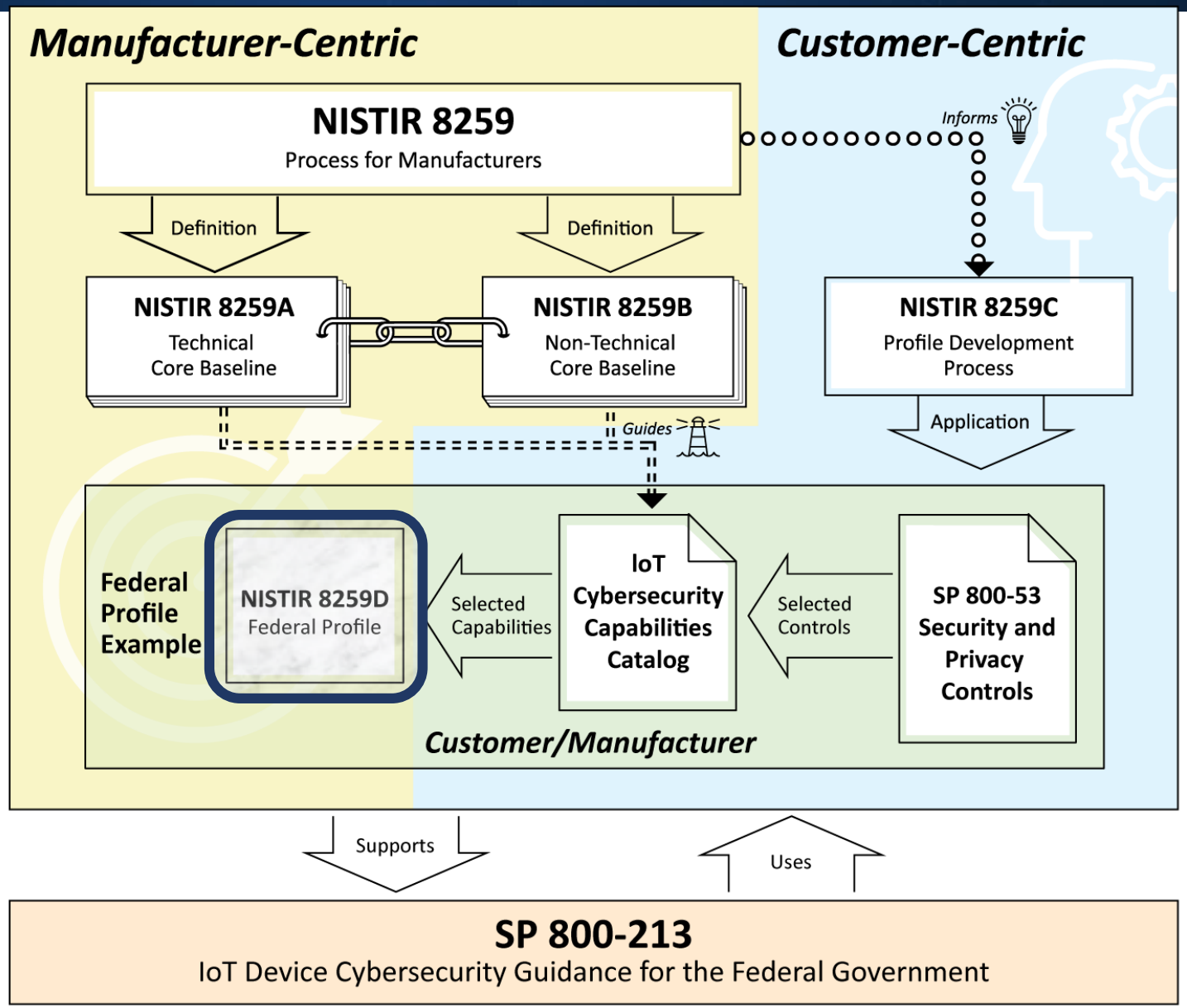
NISTIR 8259D, *Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government*

Presenter:
Barbara Cuthill

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NISTIR 8259D: Profile of the IoT Core Baseline for the Federal Government

All Of The Pieces: Four New Publications Expand Our Guidance

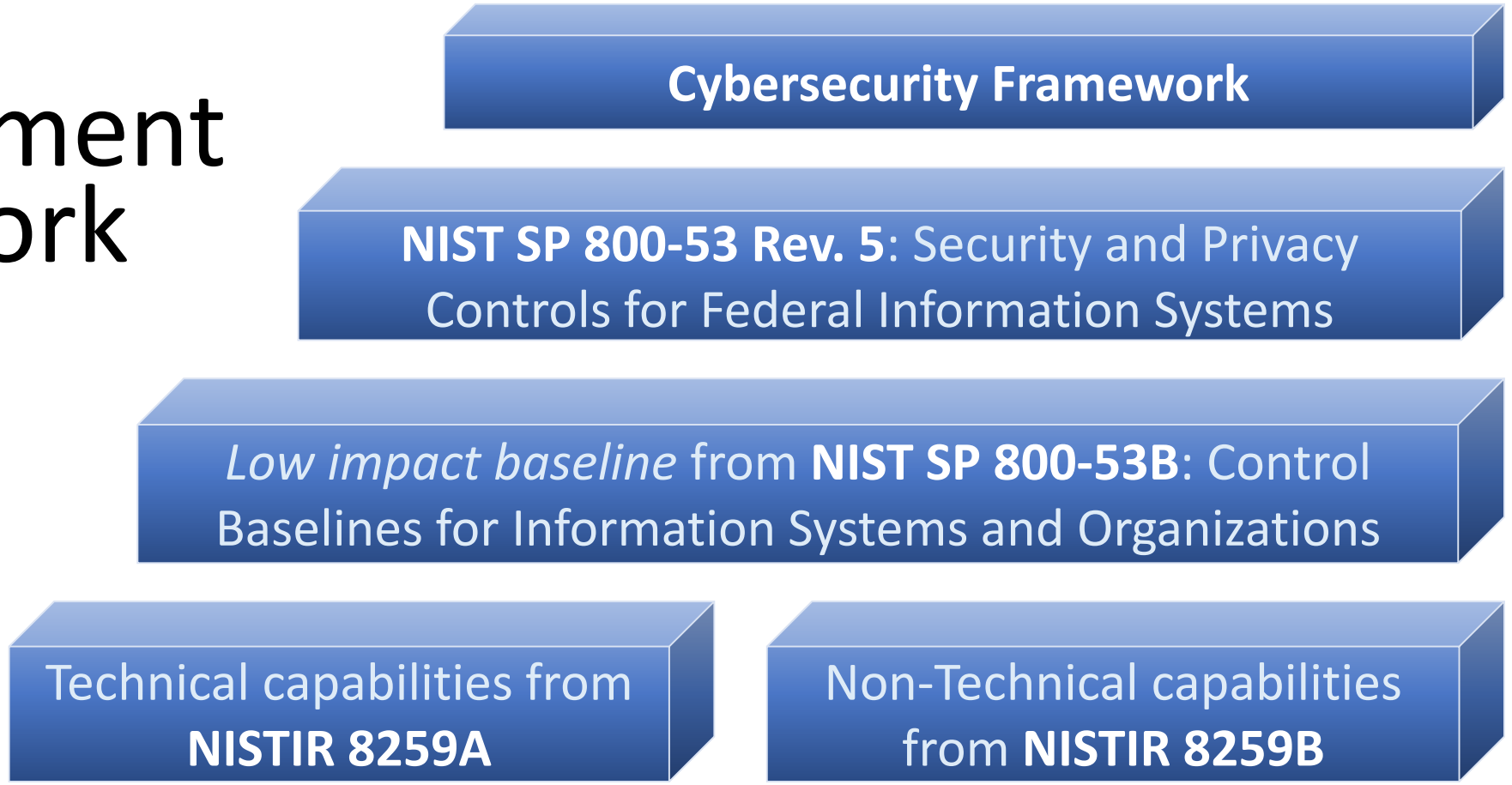


NISTIR 259C Profiling Process

1. **Identify and Gather Source Documents for Sector/Use Case Cybersecurity Requirements**
2. **Assess to What Extent the Source Documents Address the Three Concepts**
3. **Apply the Three Concepts to Source Documents to Create a Profile**
    - Analyze Source Documents Individually
    - Develop a list of device capabilities and supporting actions
    - Combine both into a coherent catalog
    - Check catalog against additional sources
    - Use minimal securability as a final filter to finalize the capabilities and actions into a profile

Step 1. Primary Source Documents

Risk Management Framework



Additional NIST Special Publications and other documents as needed

2. Assess How Documents Support…

- Device Centricity
  - Many documents are at the organization level
  - Extract device centric requirements implied by organization level documents
  - Most documents are device-neutral
- Cybersecurity-Focused Documents Selected
- Minimal Securability
  - Focus on Low impact baseline from NIST SP 800-53B: Control Baselines for Information Systems and Organizations

3. Apply the Three Concepts to Source Documents

- Device Centricity
  - Elaborated on the core baseline and non-technical baseline with a catalog of device-centric, cybersecurity-focused capabilities that would typically be needed by federal government organizations to implement 800-53 controls
  - Identified cluster of capabilities which did not fit within core technical baseline
- Focus on device capabilities needed for cybersecurity
- Minimal Securability
  - Using the controls from the low-impact RMF baseline from SP 800-53B as guidance, device cybersecurity capabilities and non-technical supporting capabilities were selected from the catalog for inclusion in the federal profile

New Capability: **Device Securability**

The IoT device can operate securely by protecting its hardware and software integrity and securely utilizing system resources, managing communications, and executing code

Table 1: Device Cybersecurity Capabilities

Capability	Sub-capabilities
Device Identification	1. Identifier Management Support 2. Actions based on device Identity 3. Physical Identifiers
Device Configuration	1. Display Configuration 2. Device Configuration Control
Data Protection	1. Cryptographic Capabilities and Support 2. Cryptographic Key Management 3. Secure Storage
Logical Access to Interfaces	1. Authentication Support 2. Authentication Configuration 3. System Use Configuration 4. Authentication Support 5. Authentication and Identity Management 6. Role Support and Management 7. Interface Control

Table 1, continued

Capability	Sub-Capabilities
 Software Update	1. Update Application Support
 Cybersecurity State Awareness	1. Access to Event Information 2. Event Identification and Monitoring 3. Event Response 4. Logging Capture and Trigger Support 5. Support of Required Data Logging 6. Audit Log and Storage Retention 7. Support for Reliable Time 8. Audit Support and Protection 9. State Awareness Support
 Device Security	1. Secure Execution 2. Secure Communication 3. Secure Resource Usage 4. Secure Device Operation

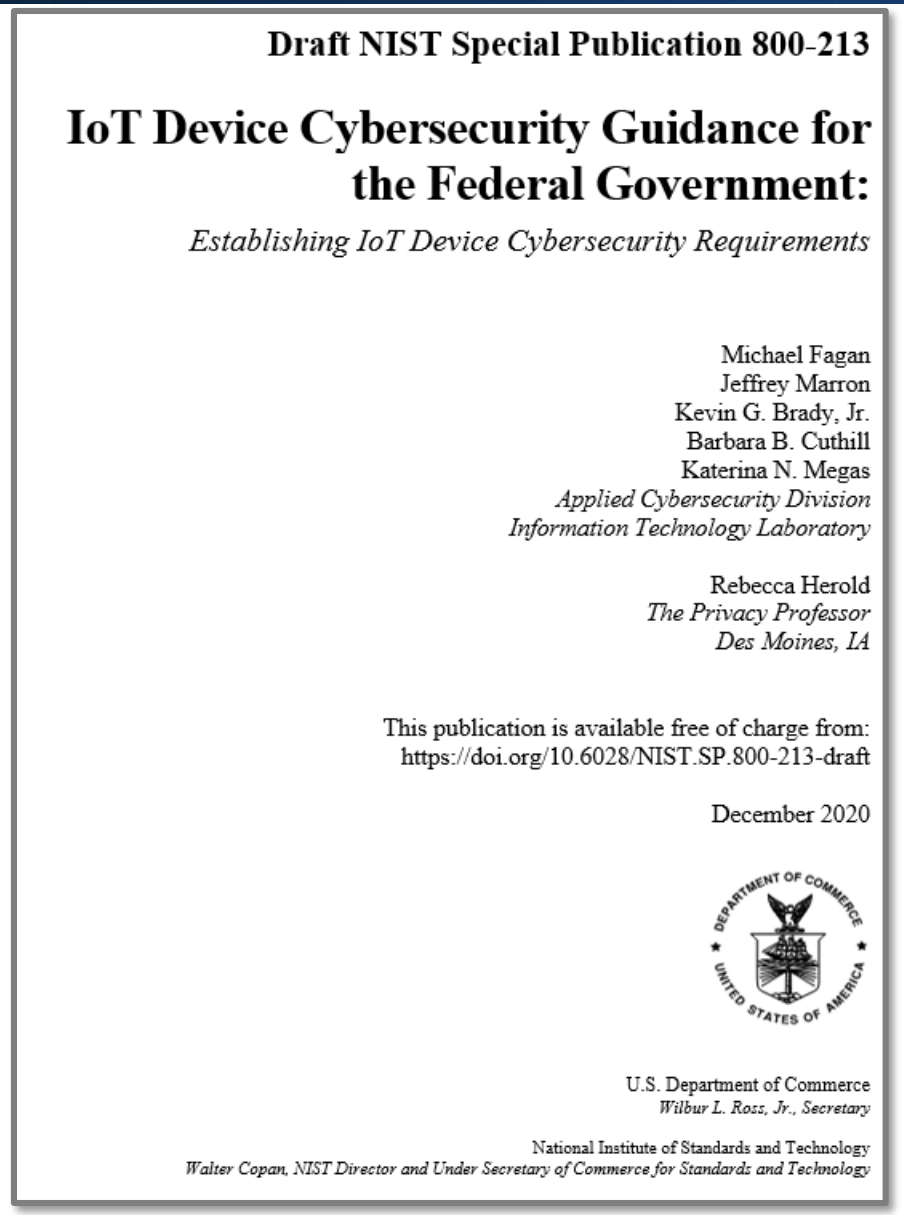
Table 2: Non-Technical Supporting Capabilities

Capability	Sub-Capabilities
 Documentation	1. Device Acquisition and Maintenance Planning Support 2. Legal Regulatory Compliance Support 3. Continuous Monitoring Support 4. Documentation for Device Cybersecurity Capabilities 5. Documentation for Post-Market Customer Activities
 Information and Query Reception	1. Cybersecurity Feature Reports and Queries
 Information Dissemination	1. Cybersecurity and Vulnerability Alerts 2. Software Update and Maintenance Notification
 Education and Awareness	1. Device Support Awareness 2. Device Cybersecurity Capability Awareness

Federal profile is a starting point.

- Assumptions made in creating the federal profile may not be sufficient to meet a specific organization's needs.
- Specific organizations may need to tailor controls and/or use common or compensating controls that may render some capabilities in the profile not applicable or insufficient to meet the specific organization's needs.
- Other organization goals beyond cybersecurity (e.g., safety, privacy, reliability, resilience) may further impact device cybersecurity requirements.

Next Up …



Draft NIST Special Publication 800-213

IoT Device Cybersecurity Guidance for the Federal Government:

Establishing IoT Device Cybersecurity Requirements

Michael Fagan
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
Katerina N. Megas
Applied Cybersecurity Division
Information Technology Laboratory

Rebecca Herold
The Privacy Professor
Des Moines, IA

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-213-draft

December 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

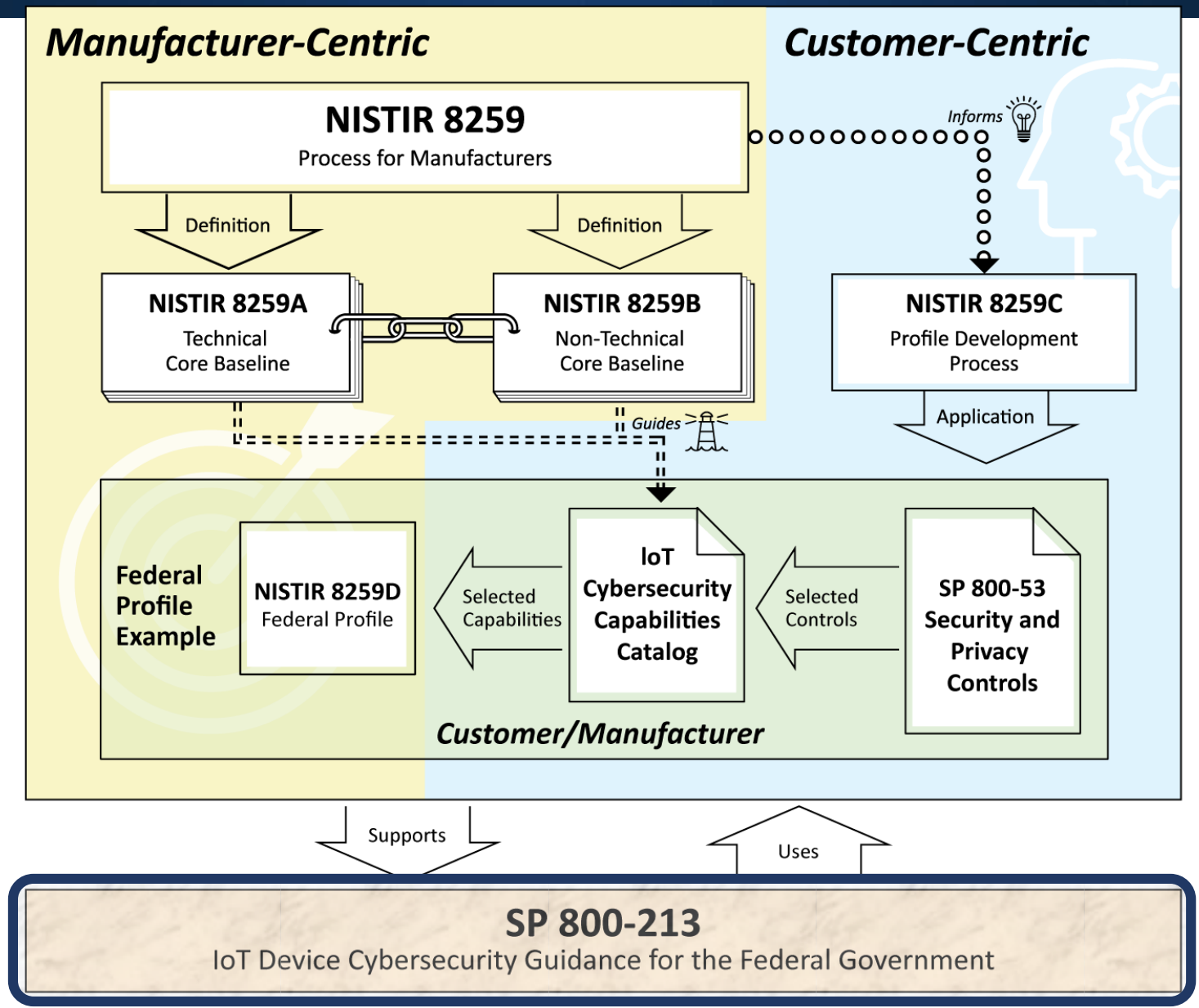
SP 800-213, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*

Presenter:
Jeffrey Marron

National Institute of Standards and Technology
U.S. Department of Commerce

Draft SP 800-213: IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements

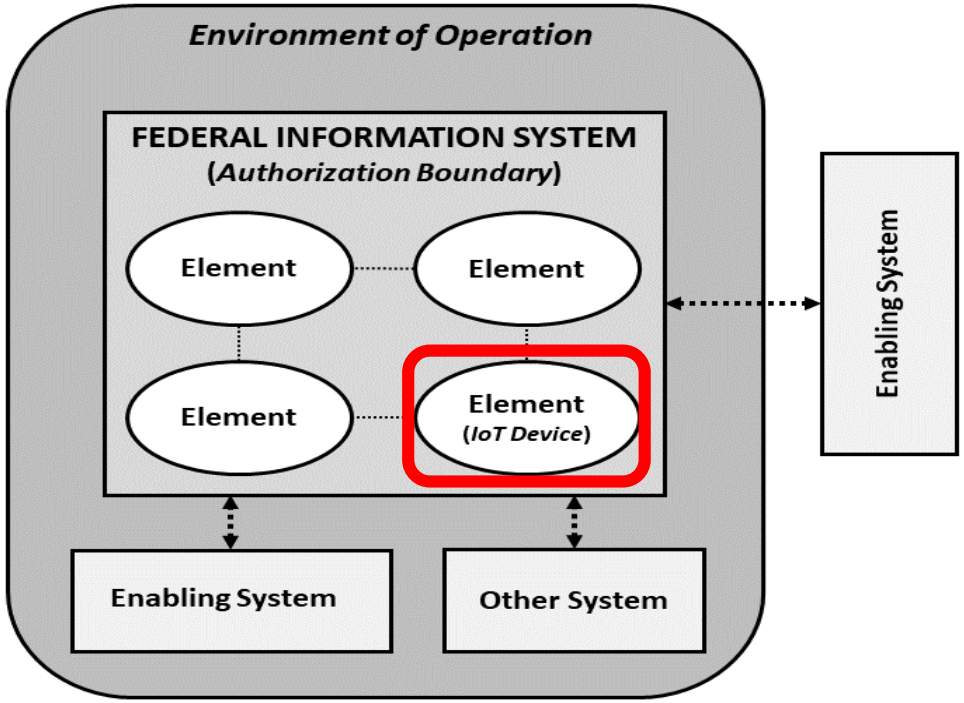
SP 800-213 In Context



Purpose of the Guidance

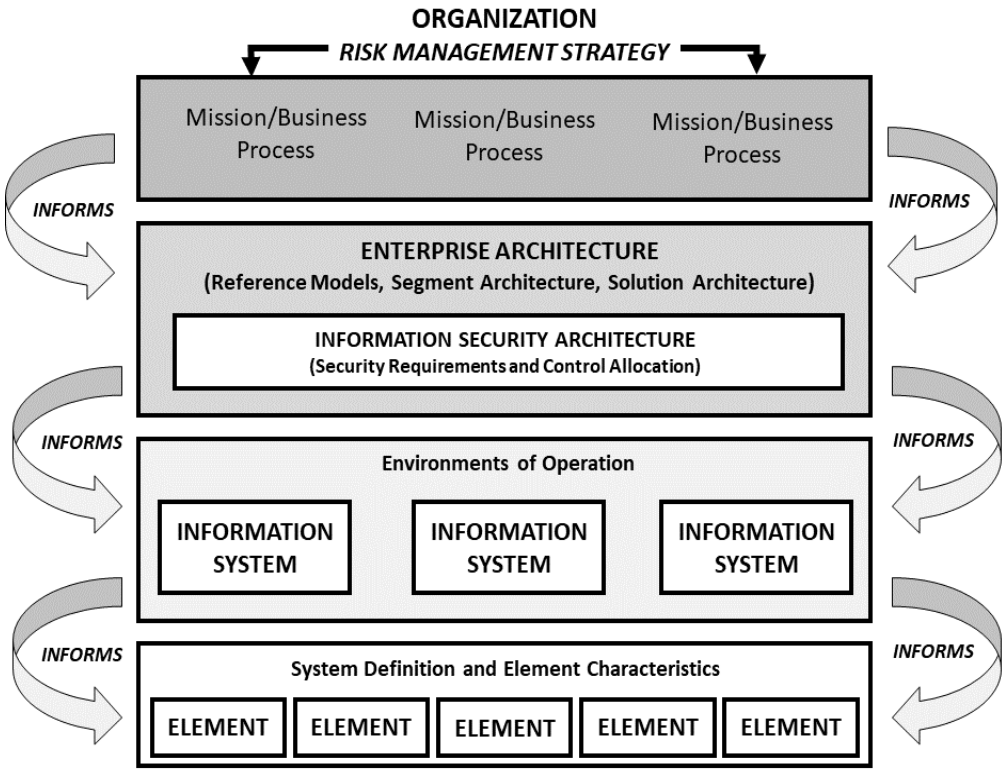
- Need to focus security requirements at the device level, below the system level
- Many IoT devices will be incorporated into existing systems with existing security controls
- Help agencies identify needed device cybersecurity requirements
- Provide guidance for agencies within the context of the Risk Management Framework (RMF)

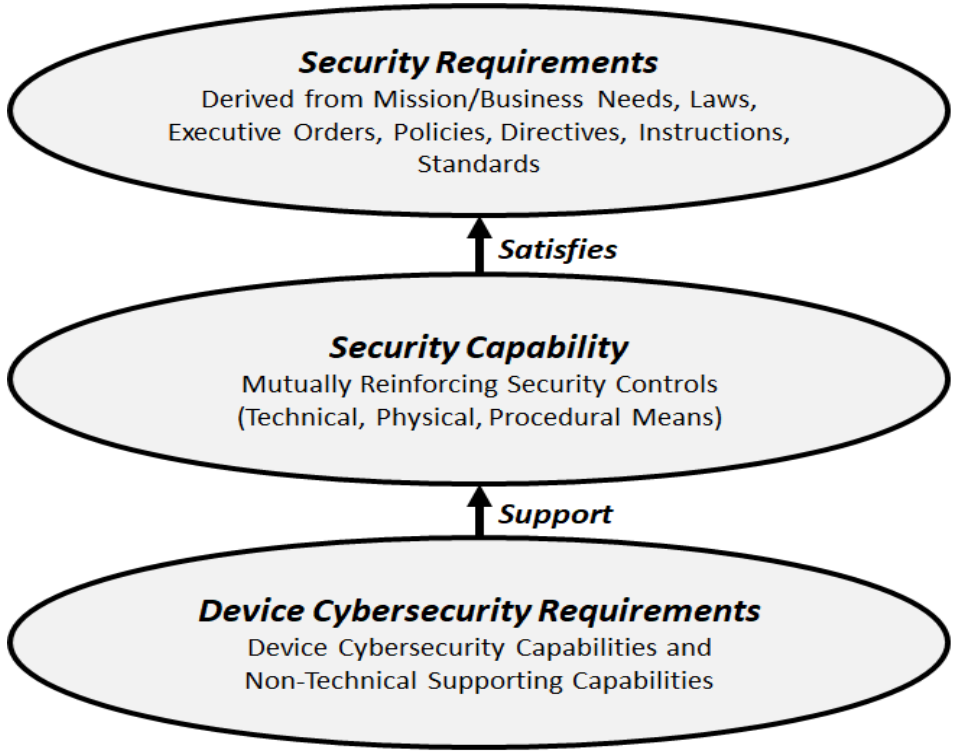
Systems and Elements



Understanding the IoT device's relationship to the information system is important to properly define the device cybersecurity requirements needed to support organizational and information system security requirements.

How IoT Devices Support Security



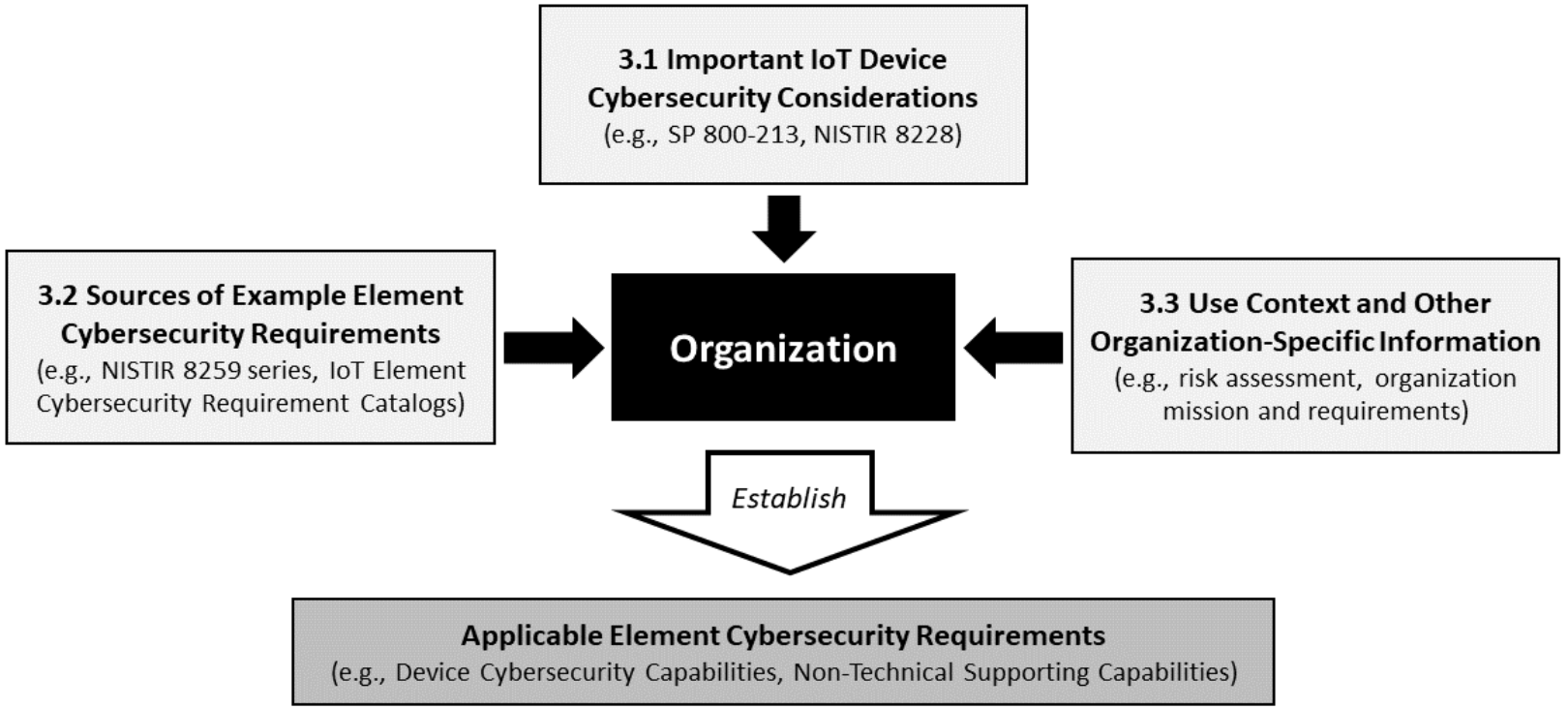


IoT device cybersecurity capabilities and non-technical supporting capabilities enable federal agencies to produce cybersecurity capabilities in their systems and organizations.

How IoT Devices May Create Security Challenges

- Many IoT devices lack features common in IT equipment
- Lack of security functionality in IoT devices could introduce unacceptable levels of risk to a system
- Apply concepts introduced in NISTIR 8228, SP 800-160
- Integration of IoT devices into existing systems can impact system and organizational security requirements

Identifying IoT Device Cybersecurity Requirements



There are multiple information sources that agencies can use to help identify device cybersecurity requirements.

3.1 Important IoT Device Cybersecurity Considerations

- What data will be collected, stored, shared?
- How will the IoT device interact with the system/org?
- Are there aspects of the IoT device and its functionality that will cause foreseeable challenges when applying security controls?
- Understanding fully the use case will help federal agencies identify IoT device cybersecurity requirements

3.2 Sources of Device Cybersecurity Requirements

- NISTIR 8259 series
- NISTIR 8259D – Federal Profile: recommended starting point for agencies to identify IoT device cybersecurity requirements
- IoT Device Cybersecurity Requirement Catalogs – both technical and non-technical capabilities
- Need to identify all applicable device cybersecurity requirements to support security controls

3.3 Use Context and Other Organization-Specific Information

- Device cybersecurity requirements identified through the guidance in Sections 3.1 and 3.2 may need tailored
- Important to identify all applicable security controls—system risk assessment may be modified
- Identify security controls that require support from system elements (e.g., IoT device)
- Translate security controls into device cybersecurity capabilities and non-technical supporting capabilities

National Institute of Standards and Technology
U.S. Department of Commerce

Wrap Up: We Want Your Feedback

Our Note To Reviewers

- **We Want Your Feedback**
  - Comments
  - Concerns
  - Clarifications Needed
- **Help Us Build Informative References**
  - NISTIR 8259B – Non-Technical Supporting Capabilities
  - NISTIR 8259D – Federal Profile
  - Use NIST 8259A as a model

Public Comment Period

- Public comments on our four new drafts will be accepted through February 12, 2021
- Send comments to iotsecurity@nist.gov

Capabilities Catalog on NIST Pages

Working to update June 2020 Catalog

Two Stages Planned:

- Stage 1: General Update, Coming Soon
  - Based on June 2020 content, restructured
  - Incorporates comments received and team analysis
  - Aligned with public drafts
- Stage 2: Incorporating Public Comments
  - Aligned with next version of December 2020 drafts
  - To be released with final versions of latest documents

Have a question or an idea? We want to hear from you!
We're always accepting thoughtful feedback at
iotsecurity@nist.gov

@NISTcyber
#IoTSecurityNIST

iotsecurity@nist.gov

https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

We welcome **your** written feedback at:
iotsecurity@nist.gov