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

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])

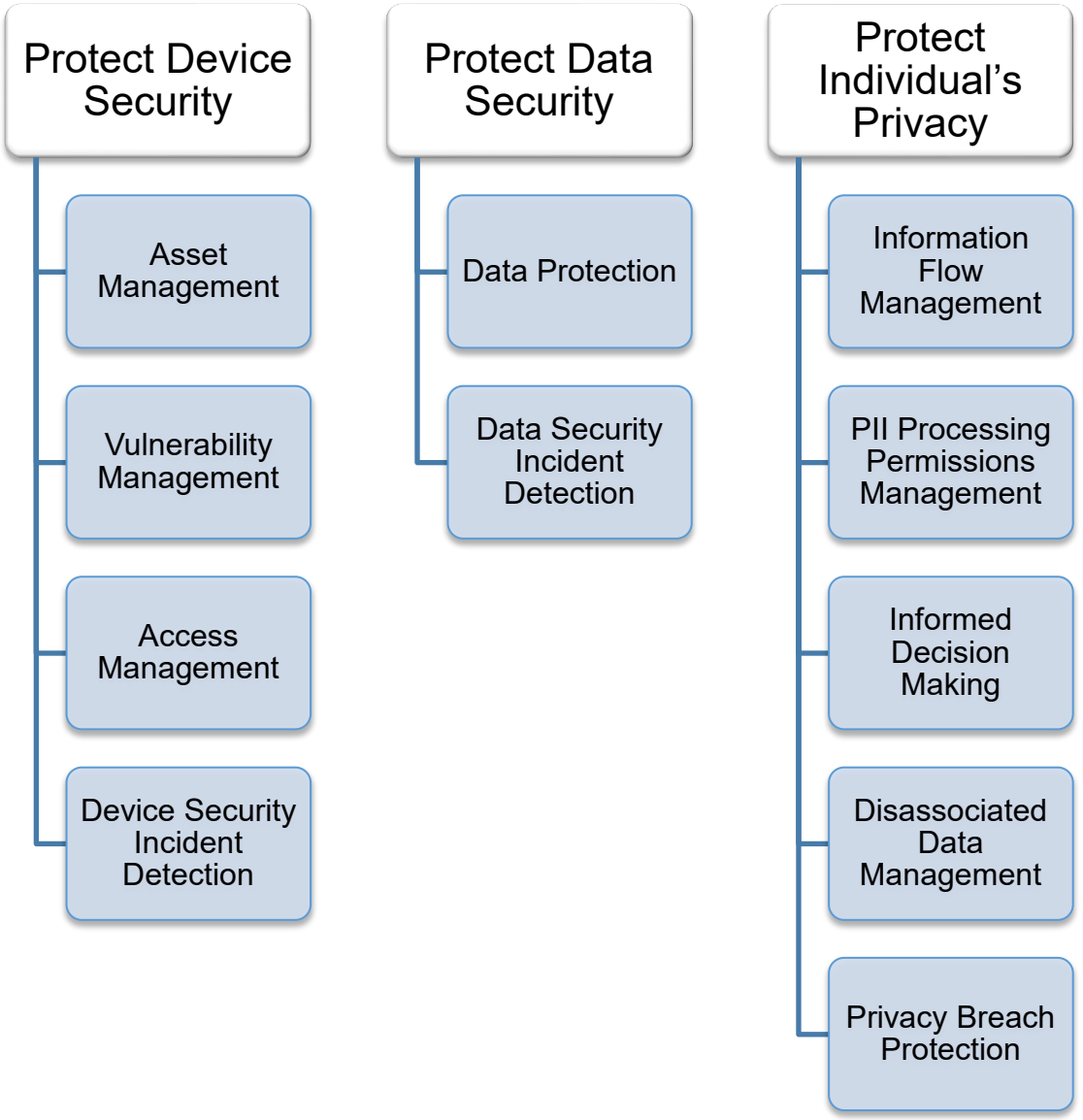
This definition is utilized in U.S. Public Law 116-207,
IoT Cybersecurity Improvement Act of 2020

IoT Potentially Introduces Unique Risks Into An Information System Environment

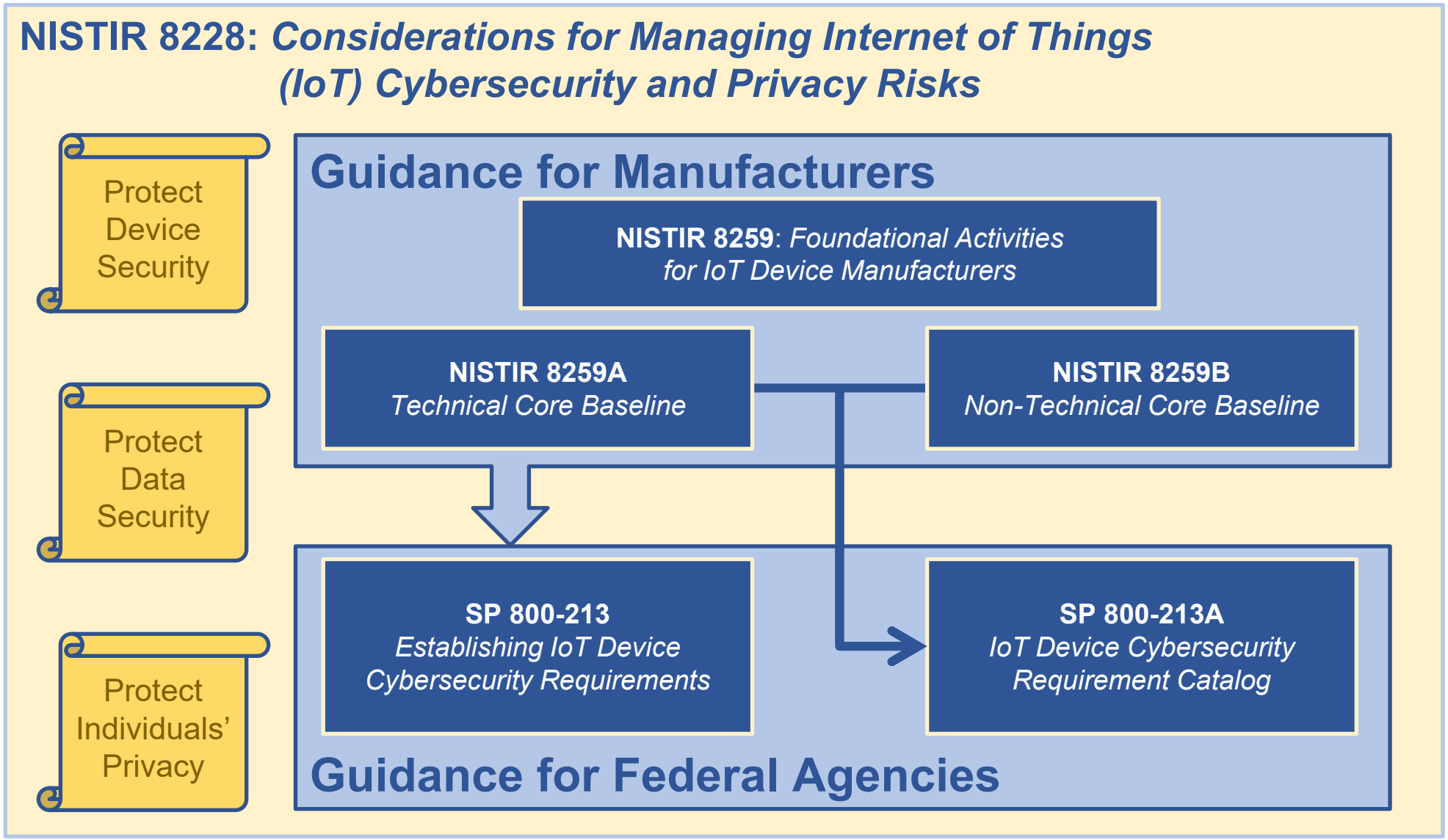
Looking through the prism of what is different about IoT:

1. Device Interactions with the Physical World
2. Device Access, Management, and Monitoring Features
3. Cybersecurity and Privacy Capability Availability, Efficiency, and Effectiveness

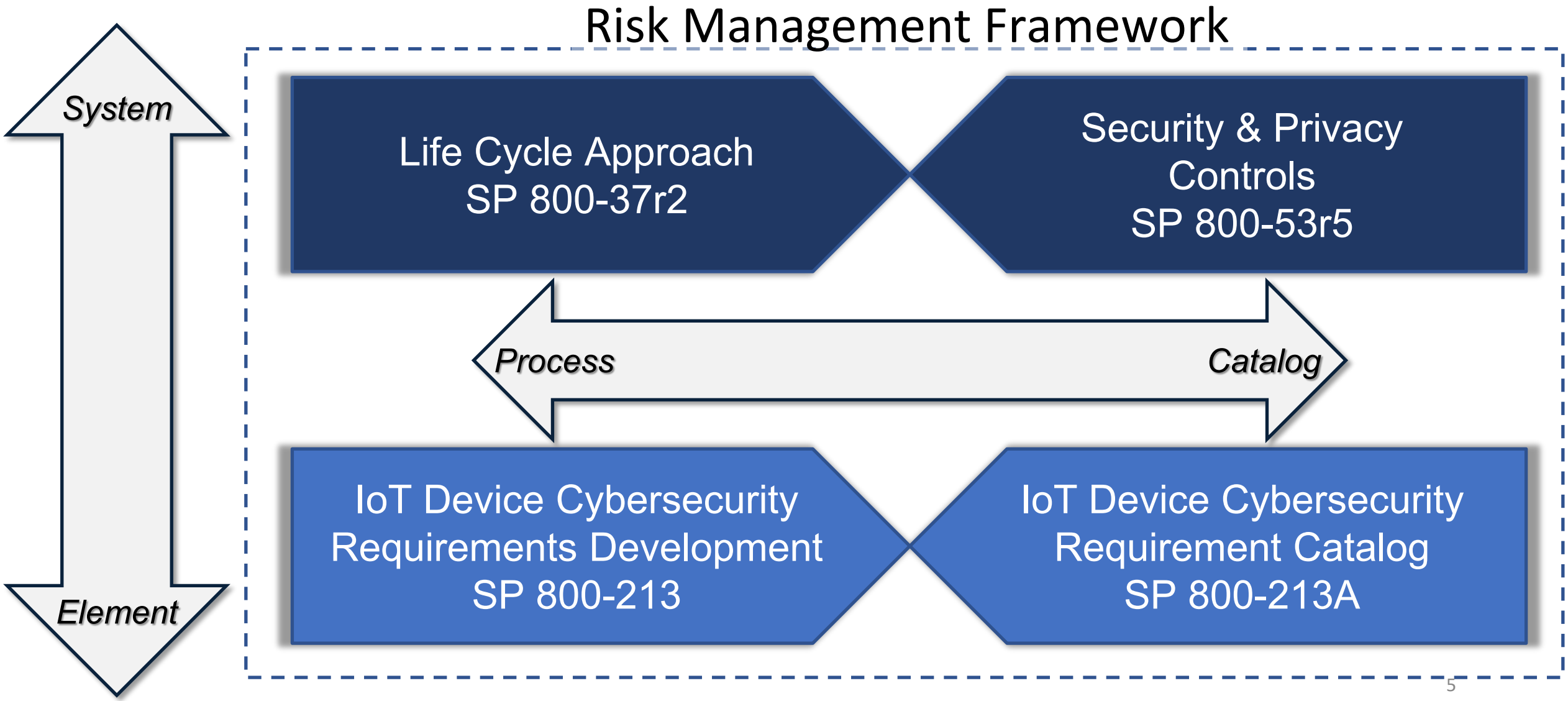
NIST identified 11 areas of cybersecurity and privacy risk management that will likely be impacted as organizations adopt IoT technologies (NISTIR 8228)



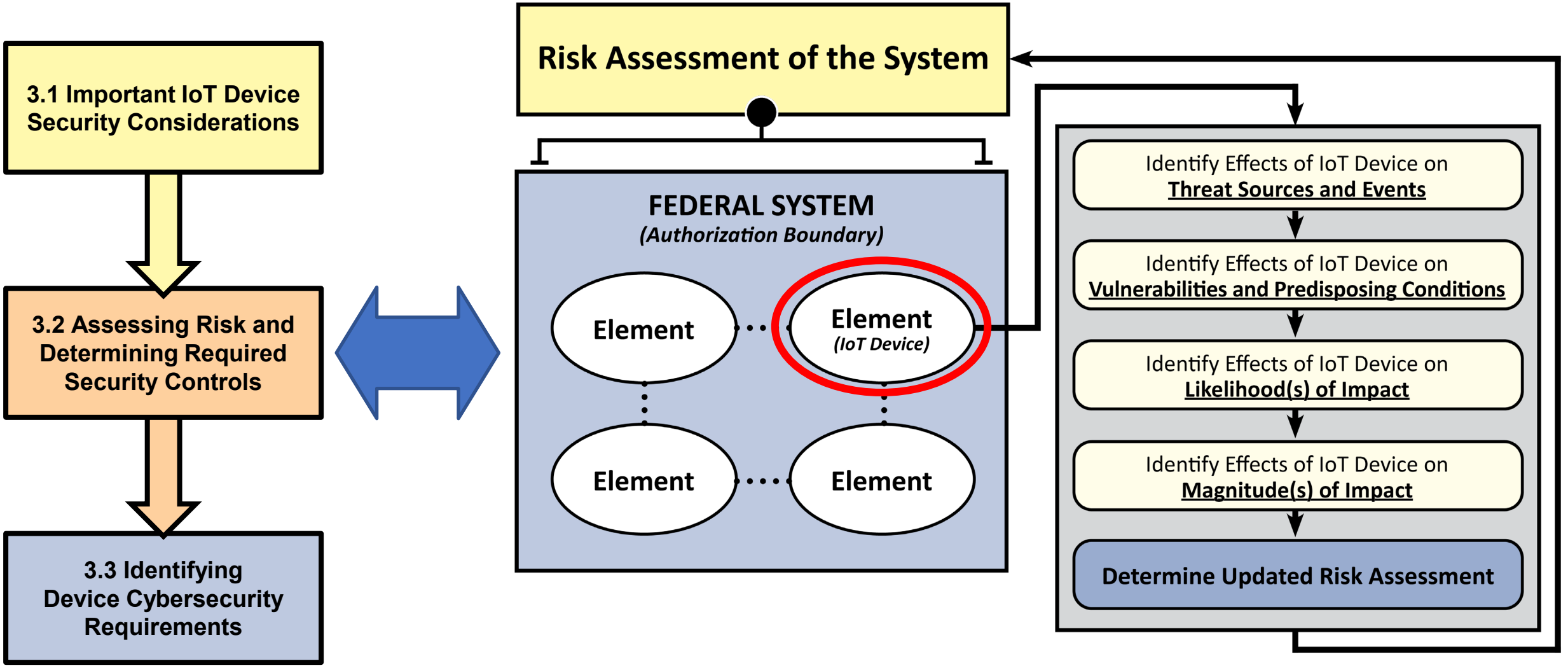
NIST Has Developed Broadly Applicable IoT Cybersecurity Guidance



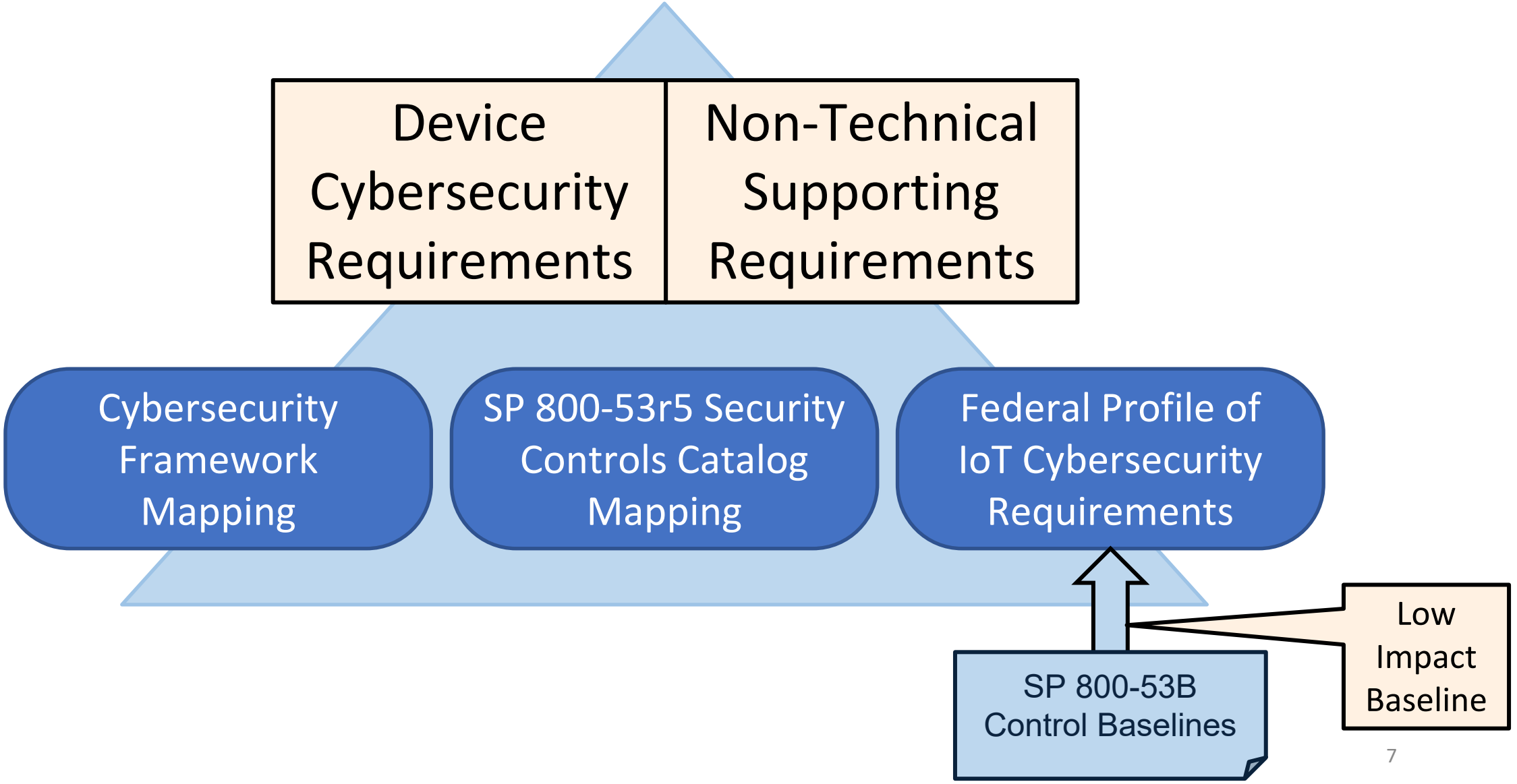
Our IoT Device Guidance Aligns With The RMF, Providing Process and Specific Controls



The SP 800-213 Process Links IoT Cybersecurity to the RMF



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



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

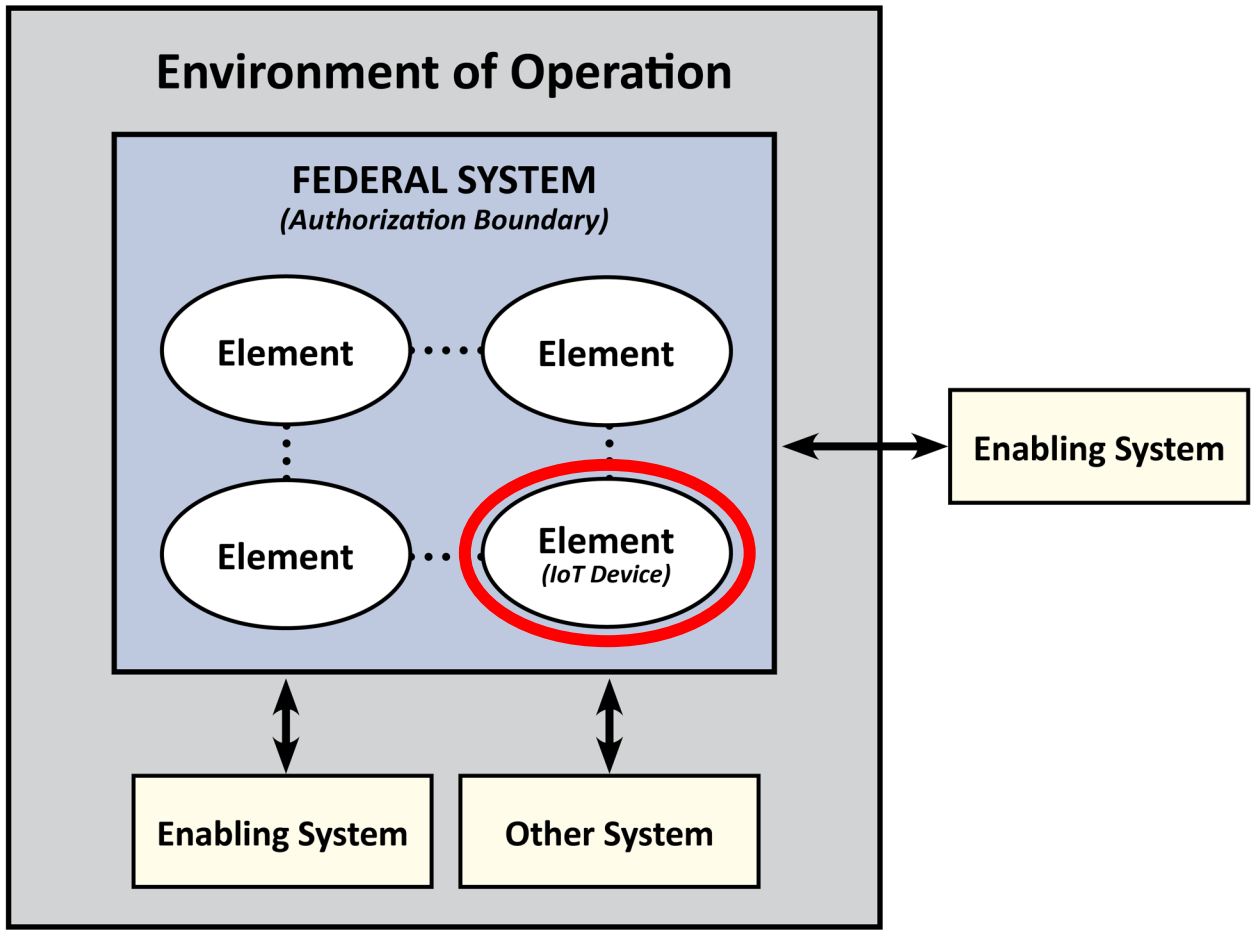
Webinar Objective: Provide an Overview of These Two Documents And Relate Them To Other NIST Guidance

SP 800-213: Establishing IoT Device Cybersecurity Requirements

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

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



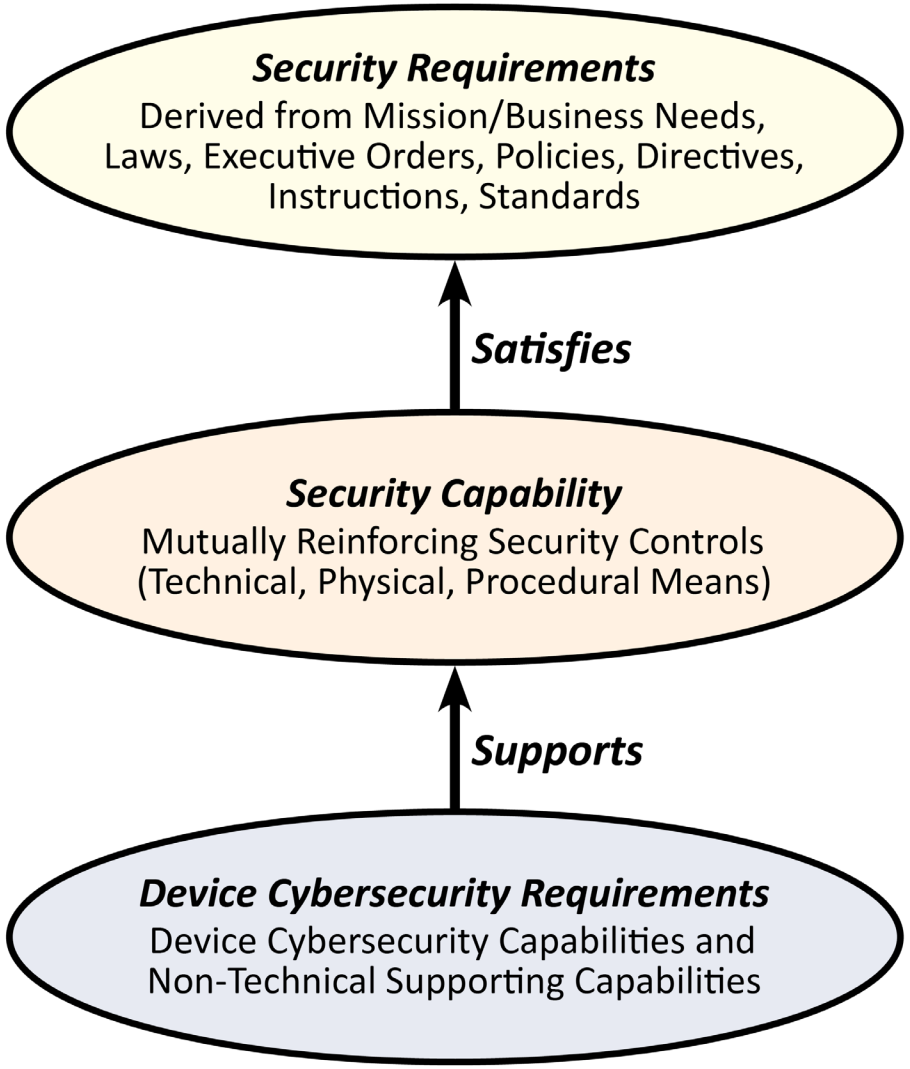
IoT Devices Can Introduce Unique Risks

- 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

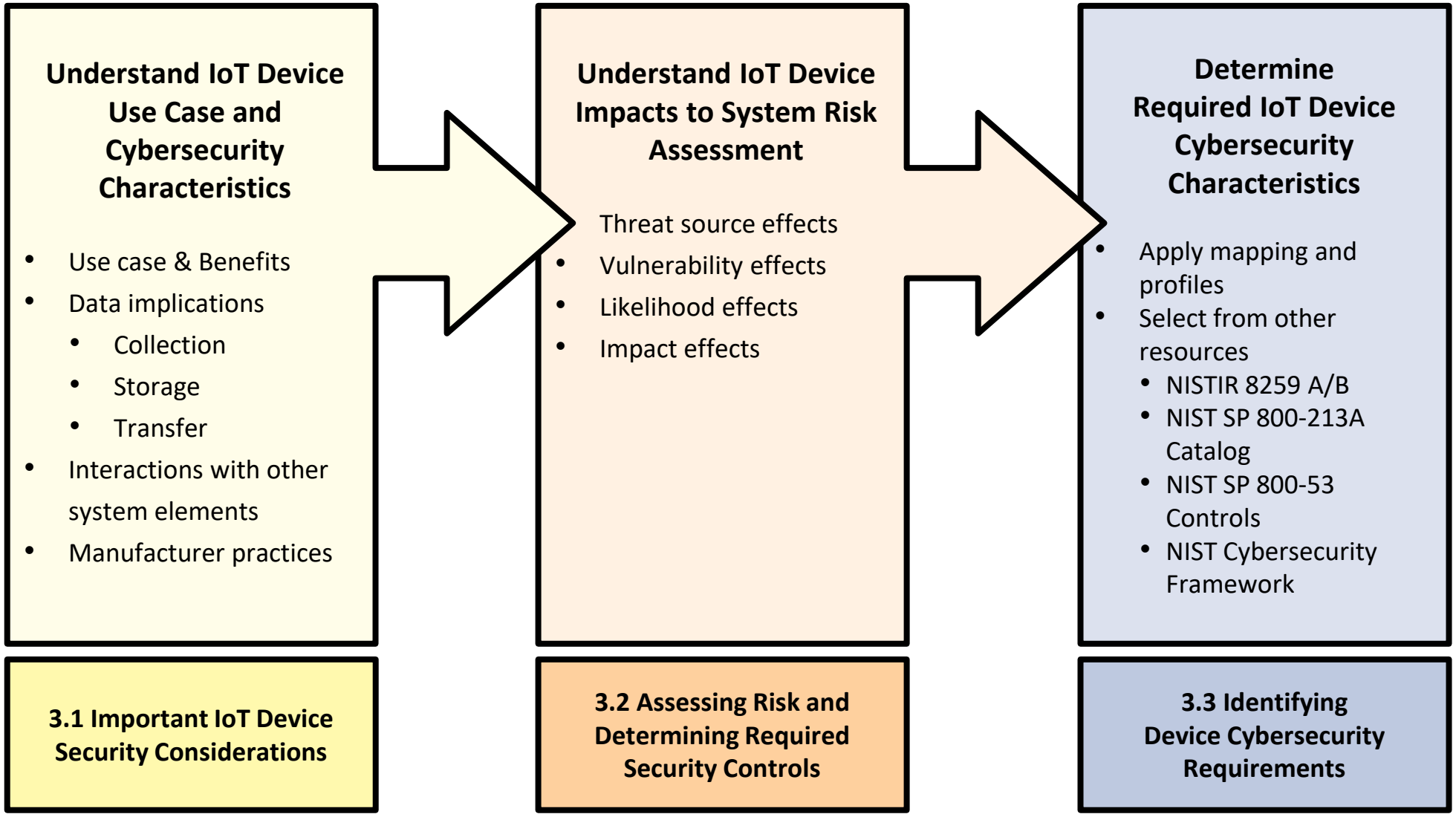
- Federal agencies must address unique risks when applying the Risk Management Framework process to systems with IoT device elements

How Components Support System Cybersecurity

- 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



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

Understand IoT Device Impacts to System Risk Assessment

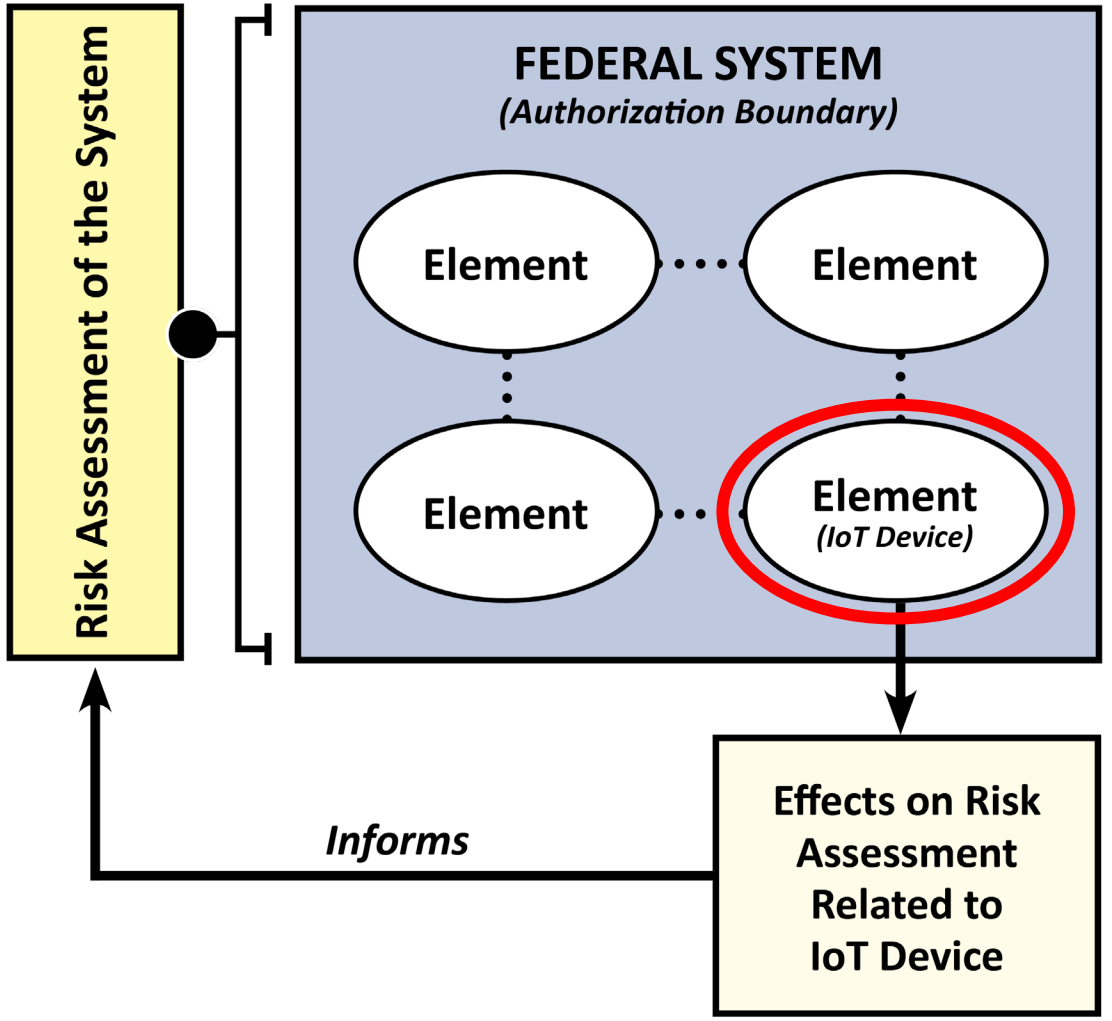
- Threat source effects
- Vulnerability effects
- Likelihood effects
- Impact effects

3.2 Assessing Risk and Determining Required Security Controls

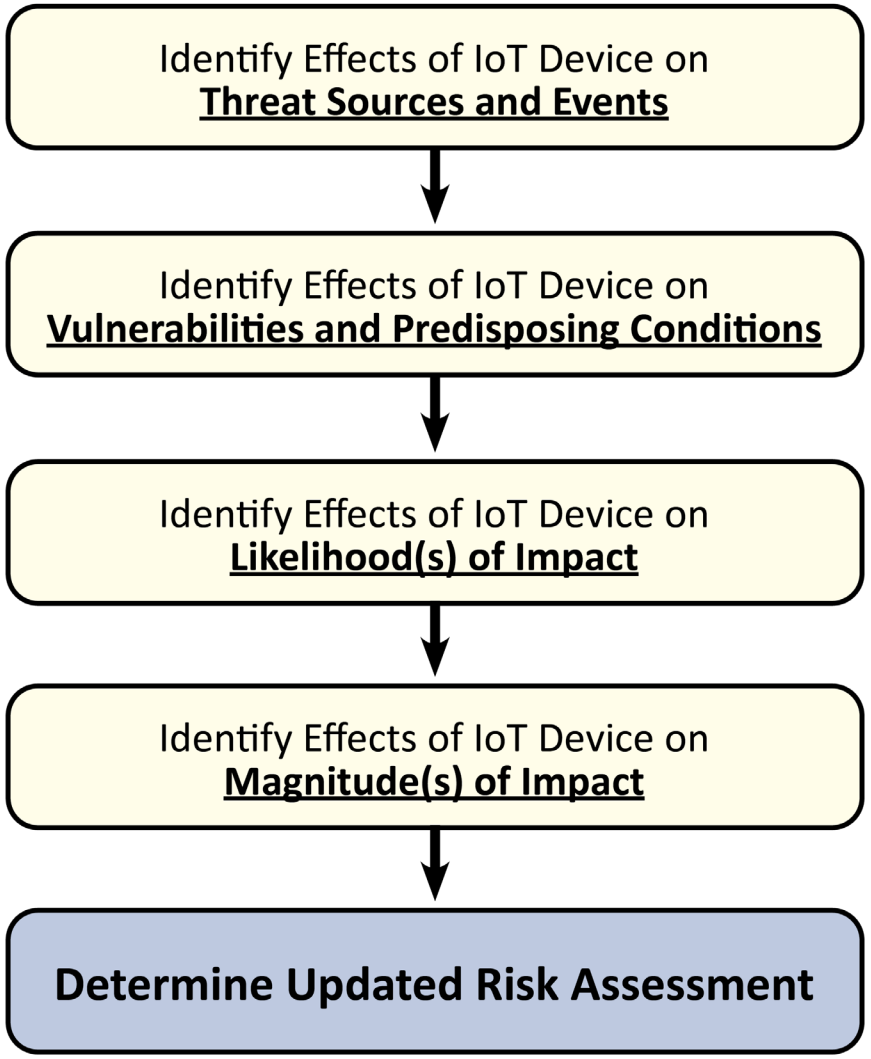
- How Does The IoT Device Affect:
  - Sources of System Threats?
  - System Vulnerabilities?
  - Likelihood of Threats?
  - Impacts of Threat Actions?

IoT Device Impacts on System Risk Assessment

- 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



IoT Device Impacts on System Risk Assessment



- 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

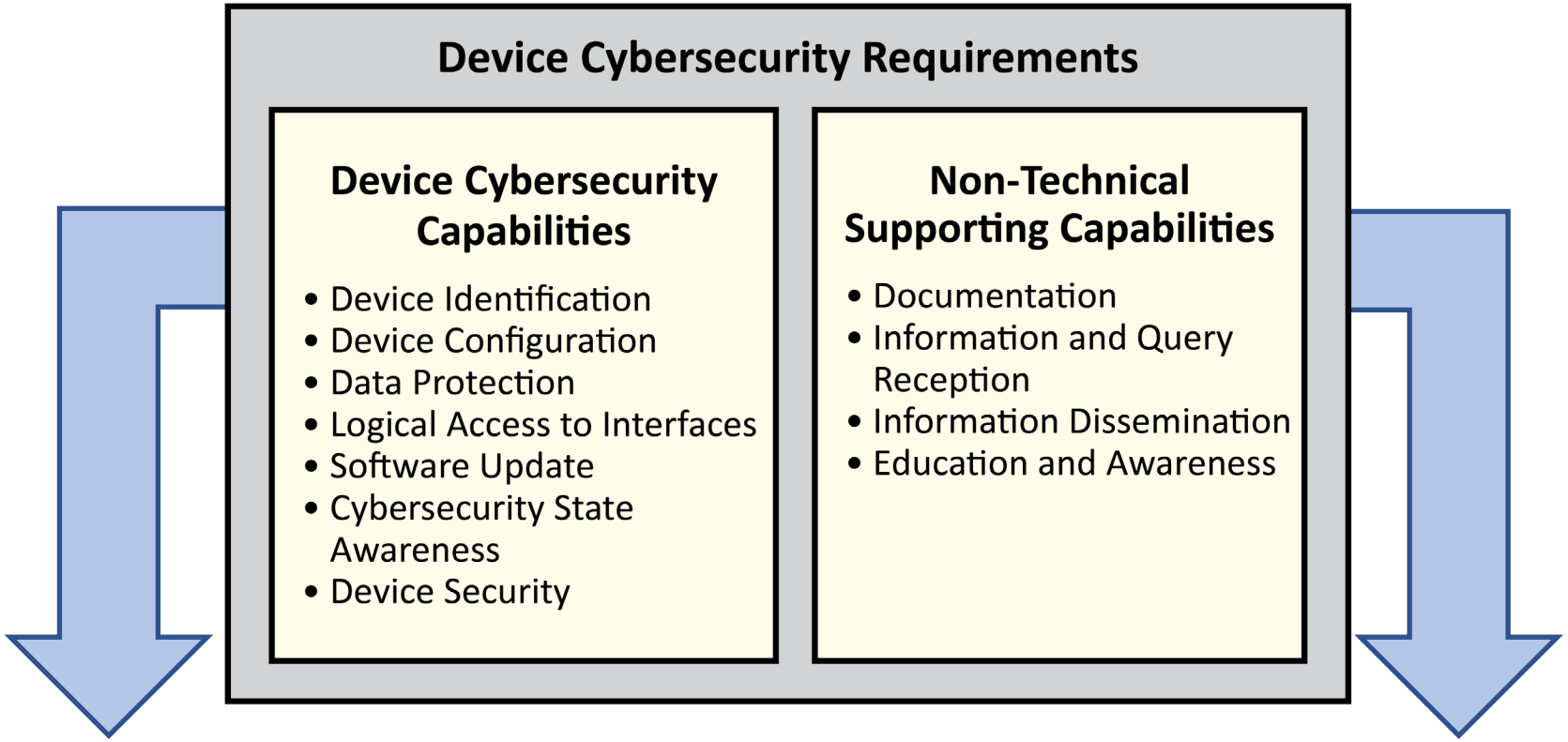
Determine Required IoT Device Cybersecurity Characteristics

- 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

- 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

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

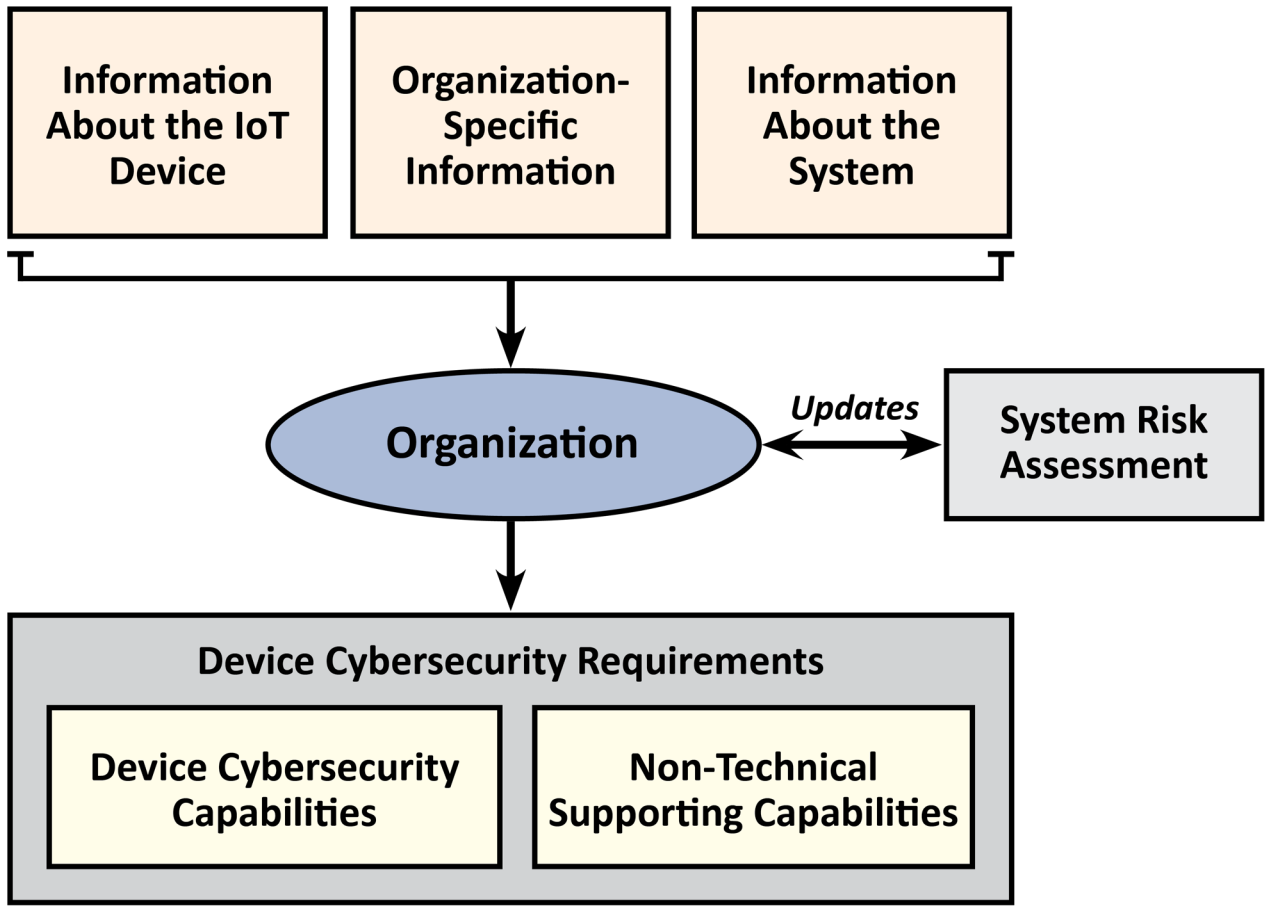


Technical support is built into the IoT device (i.e., in its own hardware and software).

Non-technical support comes from the IoT device manufacturer or supporting third-parties.

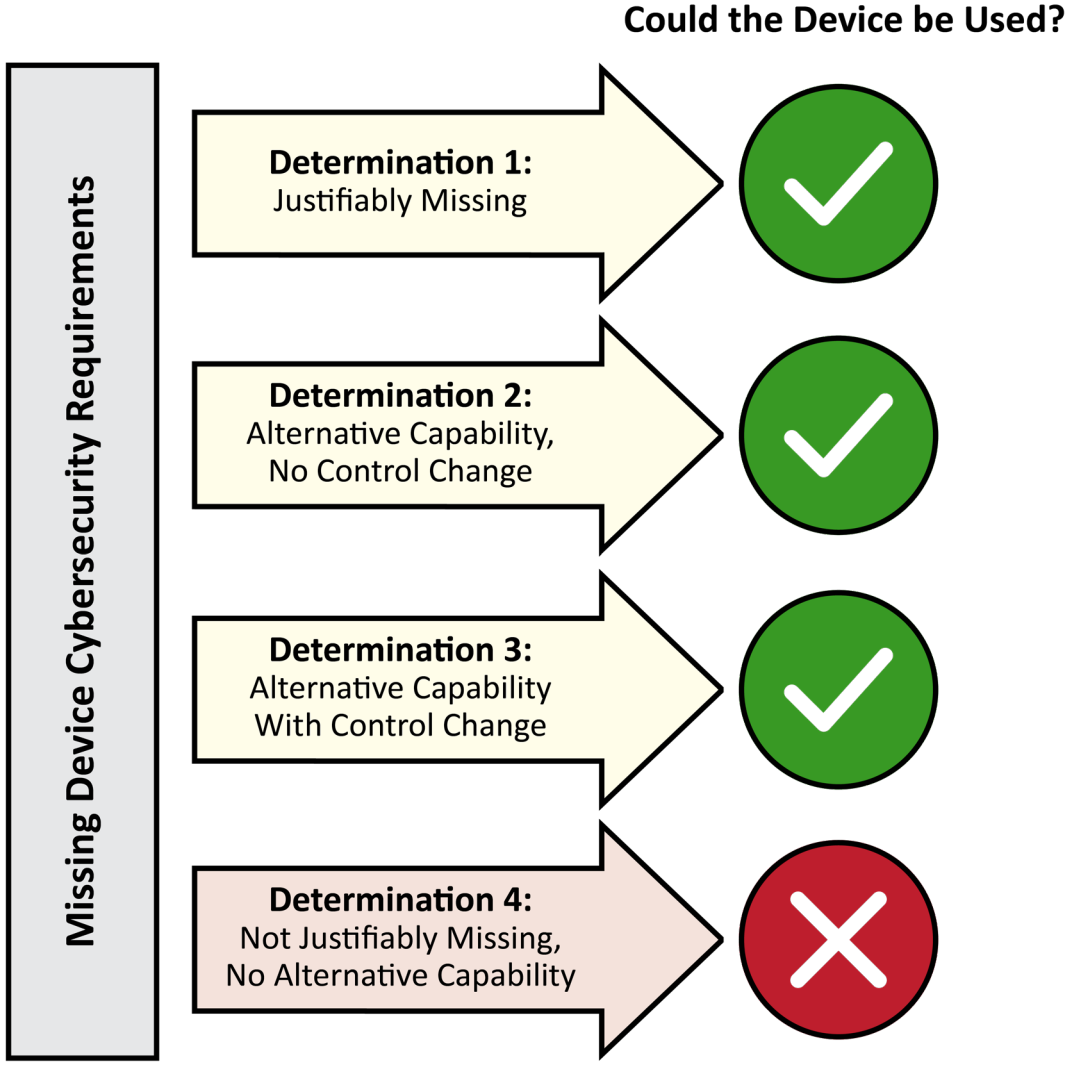
Identifying IoT Device Cybersecurity Requirements

- 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)



Addressing Missing Device Cybersecurity Requirements

- 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

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

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

  Example Capability / Sub-Capability Identifiers

- Supporting requirement have number and letter code
- Mappings to SP 800-53 and Cybersecurity Framework use complete identifiers:

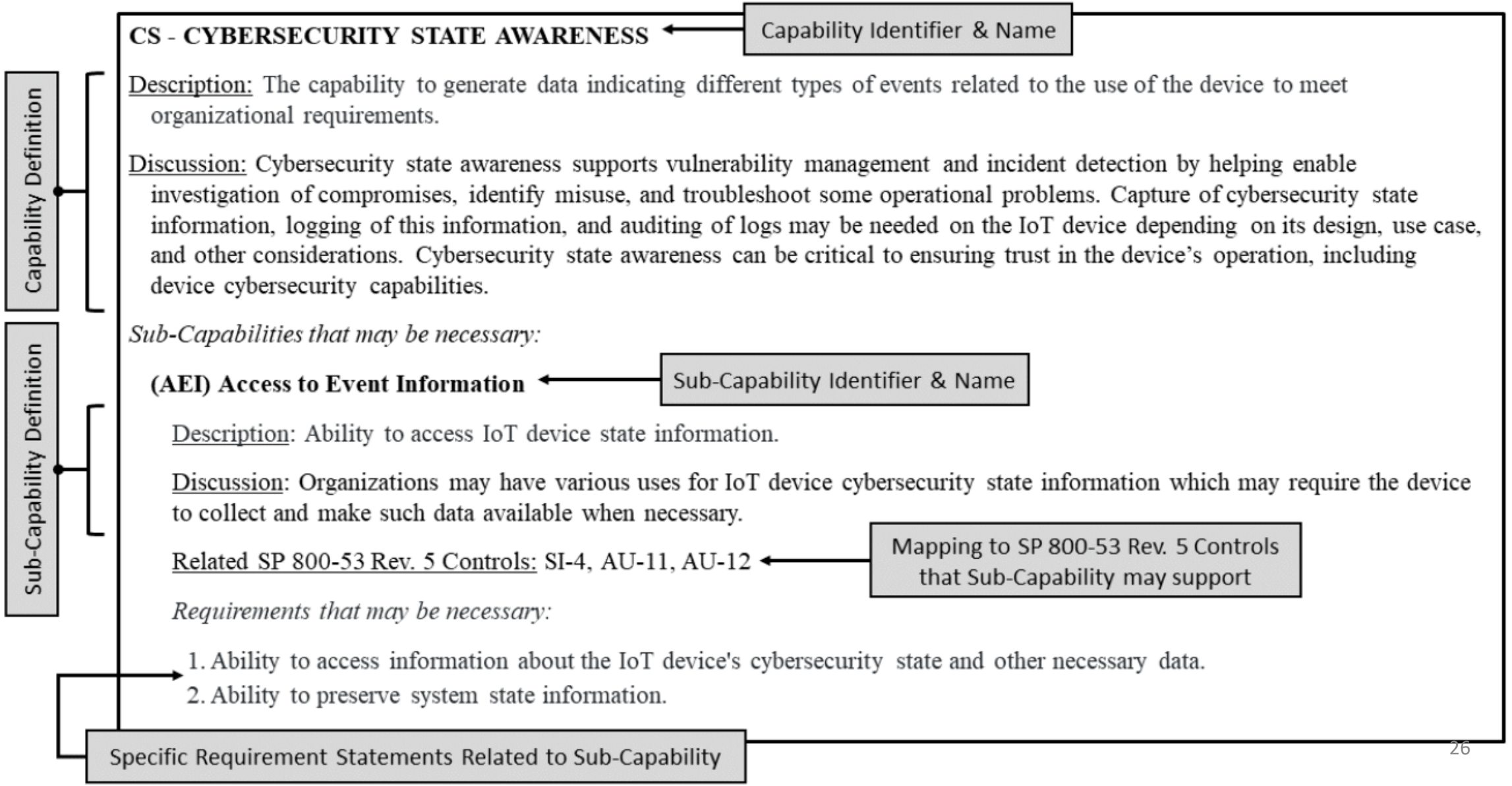
  SP 800-53 IA-3 & IA-4 map to DI:IMS(1, 2, 3)

  Example Mapping

Device Cybersecurity Capability Catalog Categories

- Device Identification (DI)
- Device Configuration (DC)
- Data Protection (DP)
- Logical Access to Interfaces (LA)
- Software Update (SU)
- Cybersecurity State Awareness (CS)
- Device Security (DS)
- Documentation (DO)
- Information & Query Reception (IQ)
- Information Dissemination (ID)
- Education & Awareness (EA)

Presentation of Capabilities in SP 800-213A: A Device Capability Example



Presentation of Capabilities in SP 800-213A: A Non-Technical Supporting Capability Example

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 **...**

Related SP 800-53 Rev. 5 Controls: CM-4(1), MA-1, PM-26, RA-9, SA-4(2), SA-10(1), SA-22, SI-2, SI-5(1), SR-8

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

Sub-Capability (requirements)	Possible SP 800-53 Rev. 5 Controls Supported
Device Identity (DI)	
Identifier Management Support (IMS) (1) (3)	IA-3, **IA-4**
Actions Based on Device Identity (AID) (2) (3) (4)	IA-3, **AC-3**, **SI-4, AU-2, CM-8**
Device Configuration (DC)	
Logical Access Privilege Configuration (PRV) (*sub-capability does not list specific requirements*)	**AC-3, CM-5**
Authentication and Authorization Configuration (AUT) (*sub-capability does not list specific requirements*)	**AC-3, CM-5**
Interface Configuration (INT) (*sub-capability does not list specific requirements*)	**AC-3**, **CM-5**
Display Configuration (DSP) (*sub-capability does not list specific requirements*)	**AC-8,** AC-12(2), AC-12(3)
Device Configuration Control (CTL) (*all requirements*)	**CM-2,** CM-3, **CM-5**, **CM-6, SR-11(2)**

Profiles are possible for many markets or product types

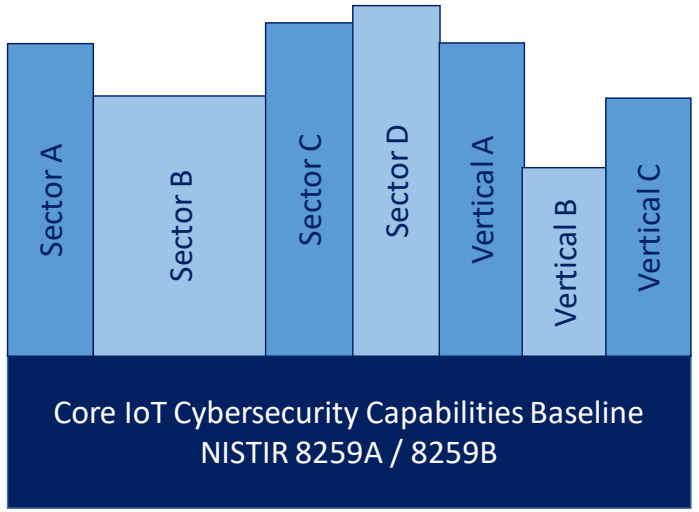
NISTIR 8259A
Technical Core Baseline

NISTIR 8259B
Non-Technical Core Baseline

SP 800-213A
IoT Device Cybersecurity Requirement Catalog

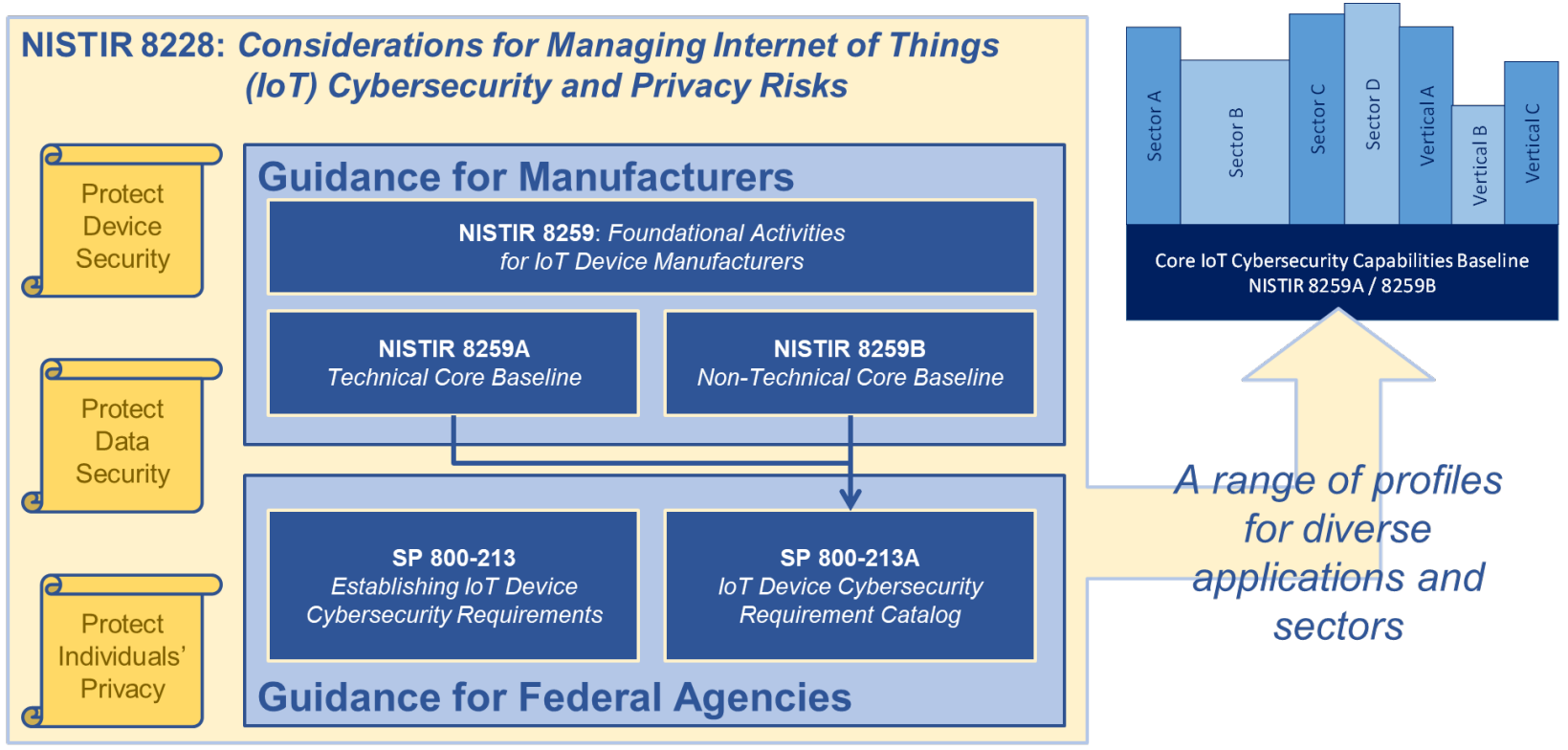
Other Standards
e.g., ETSI EN 303 645, ANSI/CTA-2088

Select / Tailor



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



Thank You!

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

Further Reading:

SP 800-213: IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements – https://csrc.nist.gov/publications/detail/sp/800-213/final

SP 800-213A: IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog - https://csrc.nist.gov/publications/detail/sp/800-213a/final

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