NIST Special Publication 800
NIST SP 800-213r1 ipd

IoT Product Cybersecurity Guidelines for the Federal Government

Establishing IoT Product Cybersecurity Requirements

Initial Public Draft

Michael Fagan
Katerina N. Megas
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-213r1.ipd

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

NIST Special Publication 800
NIST SP 800-213r1 ipd

IoT Product Cybersecurity Guidelines for the Federal Government

Establishing IoT Product Cybersecurity Requirements

Initial Public Draft

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

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-213r1.ipd

June 2026

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Arvind Raman, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST SP 800-213r1 ipd (Initial Public Draft)
June 2026

Authority

NIST Technical Series Policies

Publication History

Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added to final publication.]
Supersedes NIST Series XXX (Month Year) DOI [Will be added to final publication.]

How to Cite this NIST Technical Series Publication

Fagan M, Megas K, Marron J, Brady K, Cuthill B (2026) IoT Product Cybersecurity Guidelines for the Federal Government: Establishing IoT Product Cybersecurity Requirements. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-213r1 ipd. https://doi.org/10.6028/NIST.SP.800-213r1.ipd

Author ORCID iDs

Michael Fagan: 0000-0002-1861-2609
Katerina N. Megas: 0000-0002-2815-5448
Barbara Cuthill: 0000-0002-2588-6165
Jeffrey Marron: 0000-0002-7871-683X

NIST SP 800-213r1 ipd (Initial Public Draft)
June 2026

Public Comment Period
June 24 – August 24, 2026

Submit Comments
iotsec@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/sp/800/213/r1/ipd, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

Organizations increasingly use Internet of Things (IoT) products for the mission benefits they can offer, but care must be taken in the acquisition and implementation of this equipment. Understanding that an IoT product is a system element facilitates an understanding of how the IoT product must be considered in the risk management process. The acquisition and integration of an IoT product into an information system may alter the system's risk assessment based on new risks introduced by the product. An updated risk assessment may require additional or new controls to be selected and implemented in the system. The guidelines in this publication focus on establishing product cybersecurity requirements to support security controls. This publication provides general considerations of how IoT products may impact an information system's risk assessment and subsequent allocation of controls that may be necessary. Readers are encouraged to reference Guide for Conducting Risk Assessments, *SP 800-30, Revision 1* [3] and other publications in the Risk Management Framework (RMF) suite of publications for information on assessing risk due to the inclusion of an IoT product into an information system.

Keywords

Cybersecurity baseline; Internet of Things (IoT); securable computing devices; security requirements; product security; Risk Management Framework; Cybersecurity Framework.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication (SP) 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Supplemental Content

The NIST Cybersecurity for IoT Team has undertaken an effort that aims to help manufacturers and federal government organizations better understand the IoT product cybersecurity capabilities and supporting non-technical capabilities that may be needed from or around IoT products used by federal government organizations. To that end, NIST has developed a catalog of IoT product cybersecurity capabilities and supporting non-technical capabilities for manufacturers and IoT product customers. The catalog identifies technical and non-technical capabilities that may be necessary for supporting NIST SP 800-53 Rev. 5 [7] controls implemented in systems. Just as not every Federal Information Technology (IT) system uses every control, not every capability in the catalog is needed in every IoT product. Ultimately, the goal is to enable organizations to securely incorporate IoT products into their systems and meet their security requirements. The catalog can be found in *IoT Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog,* SP 800-213A, [18].

Note to Reviewers

This Initial Public Draft is the next step in updating SP 800-213. The authors recognize the need for this update is more than a mandate - technical, operational, and risk landscapes have each evolved over these past 5 years.

The main changes include shifting focus from IoT devices to IoT products, with language updated to be product-focused throughout. These changes are intended to clarify the difference between the 'product' and the system it is deployed within, ensure organizations consider all IoT product components, and provide organizations clarity and flexibility related to apply cybersecurity to IoT products.

The authors emphasize that the scope of this publication is focused on new IoT products – that is, considerations for those acquiring or building IoT products to integrate into their larger systems or ecosystems.

In this Initial Public Draft, the Cybersecurity for IoT Program is seeking feedback particularly on:

- Overall changes included in this draft, including the focus on product and efforts to delineate between the product and the system.
- Whether the introduced terms are clearly defined and clearly related to cyber concepts.
- Whether terms clearly relate the intended outcomes of the SP 800-213 process (i.e., IoT product cybersecurity requirements) with concepts from the RMF (e.g., security controls, security requirements)
- Review of the 'allocation' definition intended to clarify between the product and system.
- Are there any additional terms, concepts, examples, etc. that could help clarify or increase relevancy of the discussion for the intended primary audience of federal government organizations.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

    i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

    ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: iotsec@nist.gov

Table of Contents

1. Introduction ... 1
1.1. Purpose and Applicability ... 2
1.2. Target Audience ... 3
1.3. Relationship to Other Publications ... 3
1.4. Document Conventions ... 4
1.5. Publication Organization ... 4
2. Background Considerations ... 5
2.1. What is an IoT Product? ... 5
2.1.1. Network of Things ... 6
2.1.2. IoT Component Capability Model for Research Testbeds ... 7
2.2. Systems and Elements ... 9
2.3. How IoT Products Support Security ... 15
2.4. How IoT Products May Create Security Challenges ... 19
3. Identifying IoT Product Cybersecurity Requirements for IoT Products ... 21
3.1. IoT Cybersecurity Considerations ... 22
3.2. Assessing Risk and Determining Required Security Controls ... 29
3.2.1. Effects on Threat Sources and Events ... 29
3.2.2. Effects on Vulnerabilities and Predisposing Conditions ... 30
3.2.3. Effects on Likelihood(s) of Occurrence of Threats ... 31
3.2.4. Effects on Magnitude(s) of Impact of Threats ... 32
3.2.5. Determine Updated Risk Assessment ... 33
3.3. Identifying IoT Product Cybersecurity Requirements ... 33
3.3.1. Identifying Requirements using SP 800-213A ... 35
3.3.2. Identifying Requirements using Other Resources ... 36
4. Understanding Risk Management Options for IoT Products ... 38
4.1. Potential Challenges Meeting IoT Product Cybersecurity Requirements ... 38
4.2. Managing Gaps in IoT Product Cybersecurity Requirements ... 40
References ... 44
Appendix A. List of Abbreviations, and Acronyms ... 47
Appendix B. Glossary ... 48
Appendix C. Change Log ... 50

List of Figures

Figure 1 – A Network of 'Things' Modelled Using the Five Primitives [Duplicated from SP 800-183]......6

Figure 2 – Visual Depiction of the Capabilities of an IoT Component [Duplicated from IR 8316]...........8

Figure 3 - Visualization of the System and Environment 9

Figure 4 - IoT Products Represented as Enabling or Other Systems 11

Figure 5 - IoT Product Represented as a Standalone System 12

Figure 6 - IoT Product in a System Comprised of Other Subsystems 13

Figure 7 - IoT Product Components Integrated as Elements of a System..14

Figure 8 - Information Security Requirements Integration to the Element Level 15

Figure 9 - Role of IoT Product (Technical) Cybersecurity and Non-Technical Supporting Capabilities in Satisfying Security Capabilities and Requirements 17

Figure 10 - Organizations Can Use this Section to Identify IoT Product Cybersecurity Requirements ...21

Figure 11 - Steps to Updating a Risk Model and Risk Assessment using New Information about an IoT Product..29

Figure 12: Effects on Risk Assessment due to IoT Product Informs the Risk Assessment of the Entire System...33

Figure 13: Organizations Can Gather Information to Update the System Risk Assessment and Determine IoT Product Cybersecurity Requirements 34

Figure 14: Likely Outcomes for Organizations based on the Four Determinations Discussed 42

Acknowledgments

The authors wish to thank all contributors to this publication, including Danna O'Rourke Herrick and Ian Fleming, the participants in workshops and other interactive sessions; the individuals and organizations from the public and private sectors who provided feedback on the preliminary public content; and colleagues at NIST who offered invaluable inputs and feedback.

1. Introduction

IoT technology creates many opportunities for improved organizational efficiencies in support of mission objectives. Definitions of IoT vary, but there is generally agreement that IoT technology bridges operational technology (e.g., sensors and actuators) with information technology (e.g., data processing and networking).

NIST risk management guidelines help organizations identify, communicate, and satisfy security requirements to support mission and business functions and manage risk across the organization from the system level to the organizational level. As identified in NIST Special Publication (SP) 800-53 Rev. 5, security requirements are "applicable laws, executive orders, directives, regulations, policies, standards, procedures, or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted." [7] However, the increasing scale, heterogeneity, and pace of IoT deployment motivates a focus on security requirement support below the information system level, at the system element level. A *system element* is a discrete part of a system such as a device, equipment, or application that is connected to other system elements and works with them to achieve the system's goals. The IoT products and associated IoT devices organizations use will frequently be integrated as system elements; this integration will often happen well after the information system's initial deployment.

Details: What is an IoT Product?

This document uses the same definition and scope for an IoT product and device that appears in prior Cybersecurity for IoT work such as NIST Internal Report (IR) 8228 [22] and NISTIR 8259 [23]. Additional information can be found in the referenced documents and in Sec. 1.1 of this publication. NISTIR 8228 Section 2 provides additional detail on how cybersecurity capabilities are understood relative to IoT products. IoT technology may also present security challenges throughout the lifecycle if proper considerations are not made during the acquisition and integration of an IoT product. Please note, this publication will refer to both IoT devices and IoT products, but these terms are not used interchangeably. In many cases, an IoT device is related to, but distinct from, the IoT product of which it is a component.

It is important that organizations identify support for system and organizational security capabilities needed from individual system elements including IoT products to help manage risk to the federal information system. As an example, an organization may purchase voice-activated printers and integrate them into the existing enterprise network. Such voice-activated IoT products may need to access backend or cloud components for the processing of voice data and will store received voice data in those components. Organizations must grapple with the challenge that many IoT products lack features and functions that are common in conventional information technology (IT) equipment, and that data and control of the IoT product may be shared outside the traditional information system boundary. Both challenges can cause security concerns.

To help organizations with these and other IoT-related challenges, this publication provides guidelines on considering system security from the product perspective. This allows for more direct identification of needed cybersecurity requirements—the abilities and actions an organization expects from an IoT product and its manufacturer and/or third parties, respectively.

1.1. Purpose and Applicability

This publication is intended to help organizations incorporate IoT products into an existing information system as system elements. Like other NIST guidelines, *organization* describes entities of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements). A system is an interconnected set of resources that share a common functionality used or operated by an agency, a contractor of an agency, or another organization on behalf of an agency. While the term *information systems* is used in the document, the scope of the document and concerns discussed could also apply to other systems, including some operational technology (OT) systems. According to NIST guidelines [2], [3], [4], [5], [10] and FIPS 200 [21], the terms *information system* and *system* are synonymous. NIST 800-37 Rev. 2 notes that "there are many types of systems. Examples include: general and special-purpose information systems; command, control, and communication systems; … industrial/process control systems; … medical devices and treatment systems; …" [4] Therefore, most OT systems would be considered information systems as well, but the further question remains of the applicability of this publication to a specific system.

IoT products naturally bring many connections to a system through their actuation and networking capabilities. Any *system* that includes an IoT device or other IoT product component as a system element will find value in this publication. Further, the scope of this publication is focused on new IoT products – that is, considerations for those acquiring or building new IoT products to integrate into their larger systems or ecosystems. Those concerned with systems that incorporate preexisting IoT products or do not incorporate IoT products at all may find value in the guidelines within this publication as it explains how requirements for individual system elements can be identified or allocated based on system controls; some concepts and discussion may not be applicable to or align with the system of interest.

IoT products in scope for this publication have at least one IoT device and may have other system components such as additional IoT devices, one or more cloud backends, a mobile app, or a specialized hub. IoT devices in-scope for this publication have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth, Long-term Evolution (LTE), Zigbee, Ultra-Wideband (UWB)) for interfacing with the digital world. While an IoT device may be able to function on its own, it may be dependent on other product components for some functionality. While this publication might be helpful for IoT deployments that fall outside this scope or for other situations (e.g., when IoT devices are being integrated as system elements from the conception of an information system), other NIST publications, such as the Risk Management Framework (RMF) and suite of security standards and guidelines, address those situations more directly.

1.2. Target Audience

To provide guidelines in line with the IoT Cybersecurity Act, the target audience of this publication is information security professionals, system administrators, and others in federal organizations tasked with assessing, applying, integrating, and maintaining security on a system. Individuals holding the same or analogous roles in other organizations that deploy and manage systems can also use these guidelines, especially if the organization has already adopted the RMF or Cybersecurity Framework (CSF).

Personnel within the following Workforce Categories and Specialty Areas from the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity [29] are most likely to find this publication of interest as are their privacy counterparts:

- Securely Provision: Risk Management, Systems Architecture, Systems Development
- Operate and Maintain: Data Administration, Network Services, Systems Administration, Systems Analysis
- Oversee and Govern: Cybersecurity Management, Executive Cyber Leadership, Program/Project Management and Acquisition
- Protect and Defend: Cybersecurity Defense Analysis, Cybersecurity Defense Infrastructure Support, Incident Response, Vulnerability Assessment and Management

1.3. Relationship to Other Publications

This publication uses concepts from the NIST Risk Management Framework, specifically publications such as NIST SPs 800-18 Rev. 1 [2], 800-30 Rev. 1 [3], 800-37 Rev. 2 [4], 800-39 [5], 800-53 Rev. 5 [7], and 800-60 Vol. 1 Rev. 1 [10], as well as 800-160 Vol. 1 [15] and Vol. 2 [16], SP 800-82 Rev. 2 [11], SP 800-161 [17], and the NIST Cybersecurity Framework [20]. It also follows from the foundational cybersecurity for IoT work from NIST documented in NISTIR 8228 [22] and the NISTIR 8259 series [[23], [24], [25]]. Details on the relationship to these other publications are in Sec. 2.

This publication uses both the terms "security" and "cybersecurity." For most purposes, these terms are interchangeable and relate to protecting confidentiality, integrity, and availability of data. As a convention, "security" is used when discussing the protection of the system while "cybersecurity" is used when discussing how system elements might support security or protect security themselves. This mixed terminology is motivated by the common use of the term "security" in the RMF. The term "cybersecurity" is used for the same concepts in IoT to avoid confusion with physical security/safety requirements.

1.4. Document Conventions

This publication uses conventions relative to other RMF guidelines that should be understood:

This document contains guidelines for federal organizations when acquiring and/or integrating an IoT product into an existing system.

- Where the term “shall” is used, the statement is to be interpreted as a requirement.
- Where the term “should” is used, the statement is to be interpreted as a recommendation.

1.5. Publication Organization

The rest of this publication is organized as follows:

- Section 2 provides background considerations and connects the challenges presented by IoT products with risk management practices discussed in NIST publications.
- Section 3 details how the background considerations in Section 2 can be used with existing sources to identify IoT product cybersecurity requirements.
- Section 4 describes how an organization can navigate security challenges that arise when IoT products do not meet IoT product cybersecurity requirements as anticipated.

2. Background Considerations

This publication draws from other NIST guidelines, namely the Risk Management Framework (RMF) [4], the Cybersecurity Framework (CSF) [20], and *Cyber Supply Chain Risk Management Practices for Systems and Organizations,* NIST SP 800-161, [17]. Organizations familiar with these guidelines and the context of IoT products within a system could skip this section. It is expected that organizations will follow the RMF steps to manage risk throughout the system development life cycle. As IoT products are introduced to the system, sometimes after the system is in operation, it is critical to consider the security impact of such changes.

2.1. What is an IoT Product?

IoT products are systems that have at least one IoT device and may have other system components such as additional IoT devices, one or more cloud backends, a mobile app or a specialized hub. IoT devices have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth, Long-term Evolution (LTE), Zigbee, Ultra-Wideband (UWB)) for interfacing with the digital world. While an IoT device may be able to function on its own, it may be dependent on other product components for some functionality.

Using these definitions, the system that forms an IoT product is outlined that contains at least one IoT device but may also have other remote and local product components that support the IoT device's functionality. As described in *Foundational Cybersecurity Activities for IoT Product Manufacturers*, NIST IR 8259 Rev. 1 [23], IoT product components, which make up an IoT product, can contain:

- IoT devices – local equipment with at least one transducer (i.e., sensor or actuator) and at least one network interface.
- Specialty networking/gateway hardware – local equipment used to aggregate, translate, forward, or distribute data related to the IoT product across networks (e.g., a hub within the system where the IoT device is used).
- Companion application software – code executed on local equipment outside of the IoT product boundary (e.g., personal computer, smartphone) that interfaces with other IoT product components (e.g., a mobile app for communicating with the IoT device).
- Backends – remote service that supports one or more IoT product components (e.g., a cloud service, or multiple services, that may store and/or process data from the IoT device).

Some components may be clearly part of an IoT product, such as specialty networking/gateway hardware, without which IoT devices may not be able to communicate with each other or the internet. Other components may support some, but not all features, such as backends or companion application software, the absence of which may reduce functionality, but not render the IoT devices completely useless. This perspective of IoT products is based around IoT product components operating together to deliver the IoT functionality. Use of this perspective helps identify physical and logical IoT product components that can impact the cybersecurity of the IoT device or devices.

The following subsections present concepts from other NIST publications that can help readers understand IoT product system boundaries.

2.1.1. Network of Things

In *Network of 'Things'*, NIST SP 800-183 [33], the so-called Networks of Things (NoTs) are made from conceptual building blocks called *primitives* and are synonymous with IoT. The primitives discussed include:

- Sensors – electronic utilities that measure physical properties.
- Aggregators – software that implements mathematical functions to transform raw data to intermediate, aggregated data.
- Communication Channel – a medium by which data is transmitted.
- eUtility – a software or hardware product or service.
- Decision Trigger – creates the final results needed to "satisfy the purpose, specification, and requirements of a specific NoT."

In its proposed model, which is focused on data-flow, these primitives work together to create, transmit, and process data to achieve the purpose of an NoT. Figure 1, copied from SP 800-183, shows how sensors, aggregators, communication channels, eUtilities, and decision triggers can be used to model a NoT.

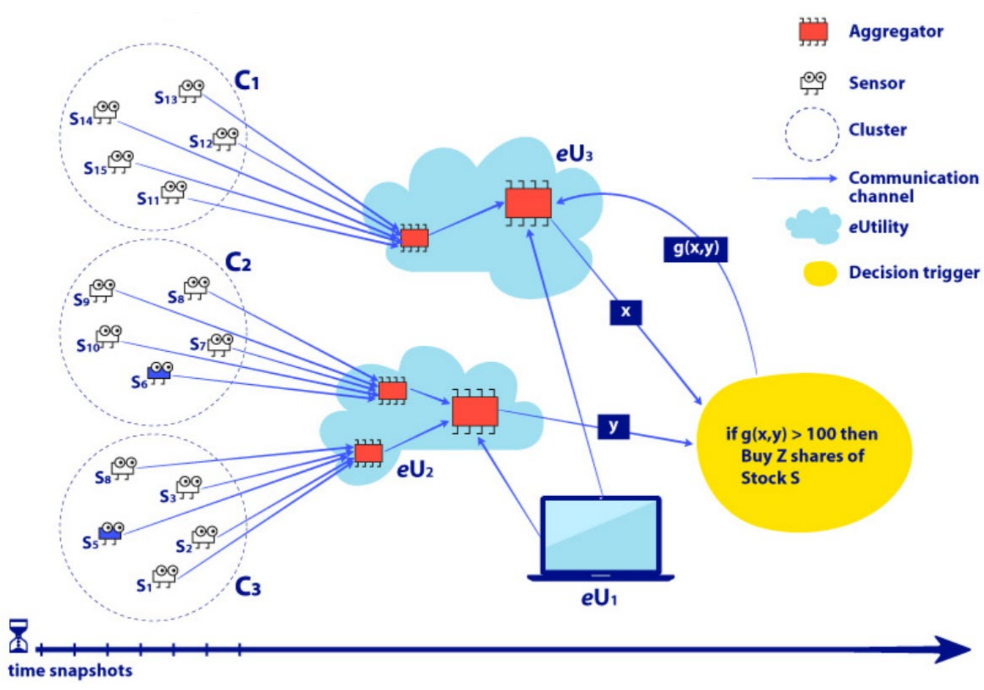

Figure 1 – A Network of 'Things' Modelled Using the Five Primitives [Duplicated from SP 800-183]

The model proposed in SP 800-183 can be helpful for some readers to understand how data flows in the IoT product they seek to use. In particular, the data flow focused model can be helpful in identifying the boundaries of an IoT product. For example, since, as SP 800-183 states, most NoTs will contain all five primitives, an IoT product can be assessed to determine if all five primitives are reflected in the data flow across all IoT product components. It is recognized that while many organizations will purchase commercially-available IoT products, other organizations may choose to assemble IoT products using available off-the shelf devices, equipment, software, and components. If the deploying organization is assembling IoT products (e.g., using off-the-shelf devices, equipment, software, and components), SP 800-183 can also help designers think through the data-centric perspective of their IoT product.

2.1.2. IoT Component Capability Model for Research Testbeds

In *Internet of Things (IoT) Component Capability Model for Research Testbed,* NIST IR 8316 [34], describes the connecting of IoT components[1] to compose IoT systems, which in turn compose IoT environments. NIST IR 8316 defines an IoT component as:

- "the basic building blocks of IoT systems" which
- "interact[s] with other IoT components to form a system" and
- "provides some function that is necessary within the system so it may achieve its goal(s)."

This definition anchors IoT components within the IoT systems they are deployed to since this definition states that IoT components provide necessary functionality for a system to achieve its goals. In this context, the IoT component capability model identifies several kinds of functions that can be used by an IoT system to achieve its goals. These capabilities are:

- Transducer capabilities – "the ability for computing systems to interact directly with physical entities of interest."
- Data capabilities – "data storing, transferring, and processing"
- Interface capabilities – "the ability to interact with other IoT components"
- Supporting capabilities – "indirectly involved in providing functionality to the system, such as monitoring, management, security, or orchestration."
- Latent capabilities – "transducer, data, interface, or supporting capabilities that are not currently enabled and accessible outside the IoT component."

Figure 2 depicts this model.

[1] *IoT components* is a distinct term from *IoT product components*. IoT components are parts of an IoT system, as defined in NISTIR 8316. IoT product components are the parts necessary to use an IoT device and constitute an IoT product as defined in this publication as well as NISTIR 8259.

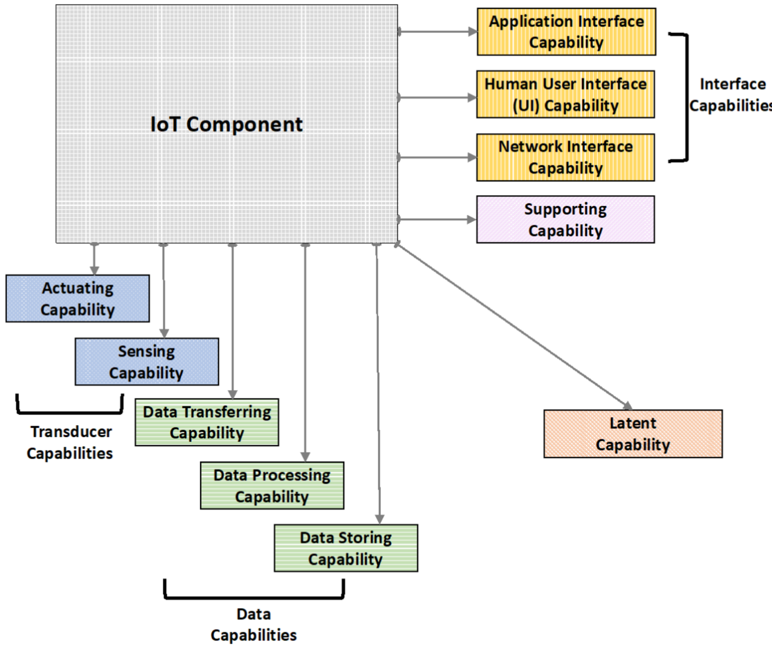

Figure 2 – Visual Depiction of the Capabilities of an IoT Component [Duplicated from IR 8316]

Though intended for use within the context of research testbeds, the IoT component capability model and its capability-focused view can be a useful perspective to complement those of this publication and SP 800-183. This model could help identify the capabilities desired from an IoT product or individual IoT product component, which can in turn inform cybersecurity capabilities needed to ensure the cybersecurity of the IoT product.

2.2. Systems and Elements

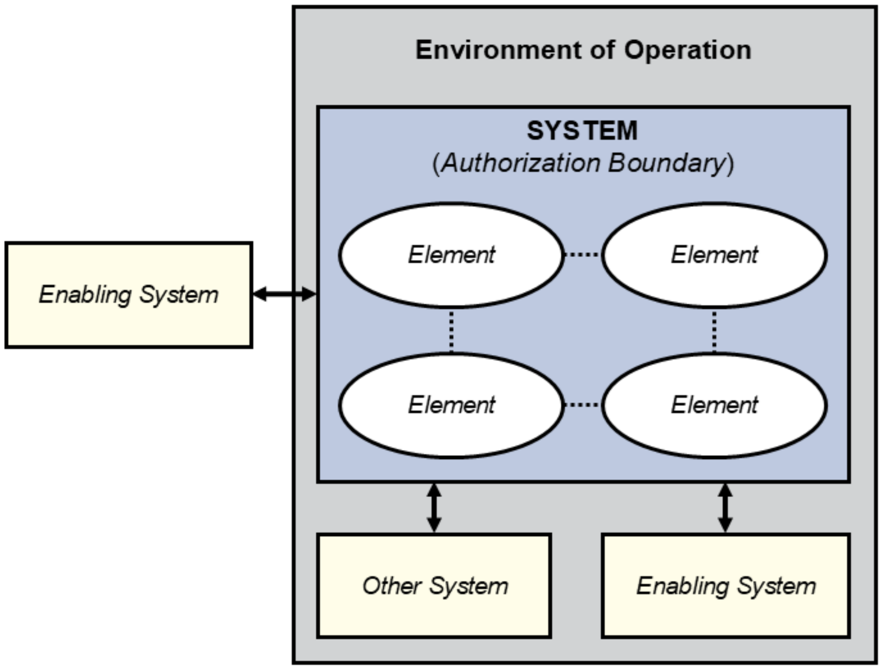

Figure 3 - Visualization of the System and Environment

As discussed in Sec. 1, federal cybersecurity risk management processes generally consider the security of organizations and systems. Further, these systems are made up of elements, which themselves are implemented with hardware and software. Increasingly, IoT devices and other IoT product components may become elements of systems. The relationship between systems and elements is a foundational concept in this publication. To understand more about this relationship between systems and elements, readers should refer to NIST Special Publication 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy [4]. Some of the key concepts, particularly those covered in Section 2.4 of SP 800-37 Rev. 2, will be highlighted here. Figure 3 shows these concepts visually, adapted from a figure in [4].

An information system "is a set of interacting elements that are organized to achieve one or more stated purposes." [28] Information systems are defined by the authorization boundary, which for systems will encapsulate elements owned and operated by organizations. The information system can also be supported by other enabling systems, which will fall outside the authorization boundary. Information systems can also interact with other systems, which might be beneficiaries of capabilities offered by the information system. The system, as defined by the authorization boundary—as well as some enabling systems and other systems—will fall within the environment of operation, which is the physical environment in which these systems reside and operate. See SP 800-37 [4], specifically Section 2.5 and Appendix G for additional guidelines on authorization boundaries for federal systems.

As explained in SP 800-37 [4], organizations define and determine the parts of the environment of operation that are within the authorization boundary of each federal system. Figure 3 shows how the environment of operation can contain multiple authorization boundaries, including other systems and enabling systems. Elements may interact and communicate across multiple systems/authorization boundaries. However, for accountability and risk management purposes, each element is only included within one authorization boundary. Each IoT device will be contained in one authorization boundary, and risk management would be handled by the organization responsible for the assigned authorization boundary. The interoperable nature of IoT and mission benefits that can come from reuse of existing equipment and deployments could create situations where the IoT device and/or its data are used by multiple systems. There may be some limited risk management responsibilities that other organizations and systems that use the IoT device and/or its data may have. For example, an urban sensor system deployed by Agency A may have benefits if the data it creates was used by a system deployed by Agency B. Though the IoT devices in the sensor system would be within an authorization boundary managed by Agency A, Agency B may allocate security requirements and have to implement controls around their use of the sensor system's data to meet government-wide requirements. *Allocation* refers to "the process an organization employs to assign security or privacy requirements to an information system or its environment of operation; or to assign controls to specific system elements responsible for providing a security or privacy capability (e.g., router, server, remote sensor)." [4] Allocation is pertinent to this publication since the fact that security requirements are allocated to IoT products and IoT product components is a core motivation of the guidelines provided. In other words, this publication is aimed at helping organizations manage the allocation of security requirements to IoT products.

The concept of systems and elements can help clarify the ways IoT products and their comprising IoT product components might be conceptually viewed by organizations to support the identification and allocation of product cybersecurity requirements. Considering that IoT products are usually comprised of multiple IoT product components and can include IoT devices, companion software applications, specialty network hardware (which can be considered distinct from IT network infrastructure), and remote services, organizations have flexibility in how they assemble elements into systems and subsequently draw authorization boundaries. Organizations therefore also have flexibility in conceptually viewing how IoT products and product components are added to their systems.

Relative to other systems managed by the organization, some IoT products should be characterized as an "enabling" or "other" system if its component IoT device and other IoT product components is managed in a different authorization boundary than the organization's system. As discussed in SP 800-37 [4], an enabling system is one that "may provide common controls for the system or may include any type of service or functionality used by the system," and other systems as those "also outside the authorization boundary and may be the beneficiaries of services provided by the system or may simply have some general interaction." SP 800-37 [4] goes further to note that the risk management of these kinds of systems would be "addressed within their respective authorization boundaries." An example of this type of other system might be a building or campus monitoring system that is primarily autonomous. Such a system will mainly benefit from some of the federal system's capabilities (e.g., an internet connection, access to data within the authorization boundary), while implementing its own security controls. Figure 4 shows how an IoT product can be visualized relative to a system and how they can exist as enabling or other systems within or outside the environment of operation. Note in this case the IoT product is placed clearly outside the authorization boundary.

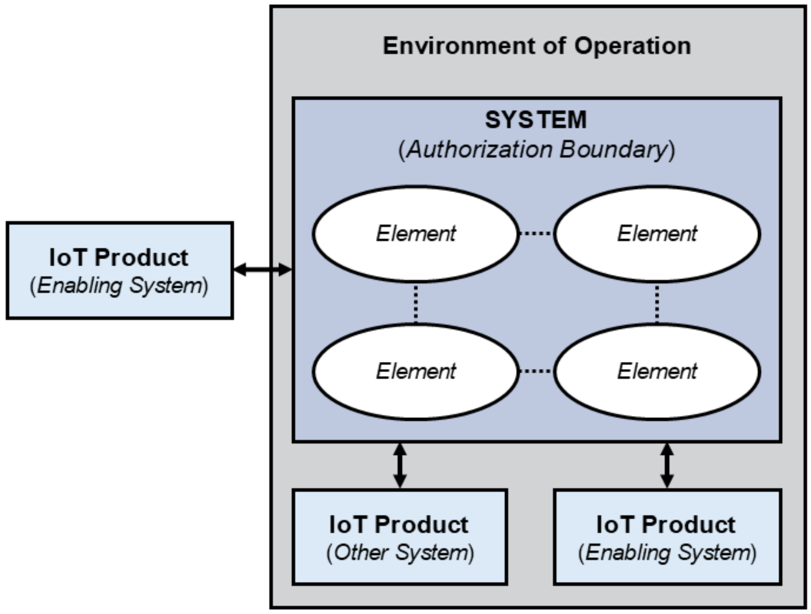

Figure 4 - IoT Products Represented as Enabling or Other Systems

Consider: Cybersecurity Responsibility Related to *Enabling* and *Other* Systems

Considering an IoT product as an *enabling* or *other* system does not alleviate all cybersecurity considerations on the part of an organization. The IoT product will still exist in another authorization boundary, which may or may not be managed by organizations that do not necessarily use the RMF (e.g., the product manufacturer, third-party service provider). That organization (i.e., that manages the IoT product within their authorization boundary) would have to be responsible for many aspects of risk management related to the IoT device, but any organization that uses the IoT device directly, services it provides, and/or its data will have responsibilities related to cybersecurity of that IoT device and its data. Readers of this document should refer to NIST *Cyber Supply Chain Risk Management Practices for Systems and Organizations,* SP 800-161 Revision 1, [17] to understand these responsibilities and supporting practices.

Many IoT products will require some integration and management by the customer organization, and so IoT products may also be placed inside the authorization boundary as a subsystem. In this context, organizations can still view the IoT product and its components as a standalone system, but now there will likely be different implications for cybersecurity and the organization that will come with placement within the authorization boundary. Figure 5 shows how an agency can visualize this scenario for an IoT product comprised of an IoT device, companion application, specialty networking hardware, and remote service.

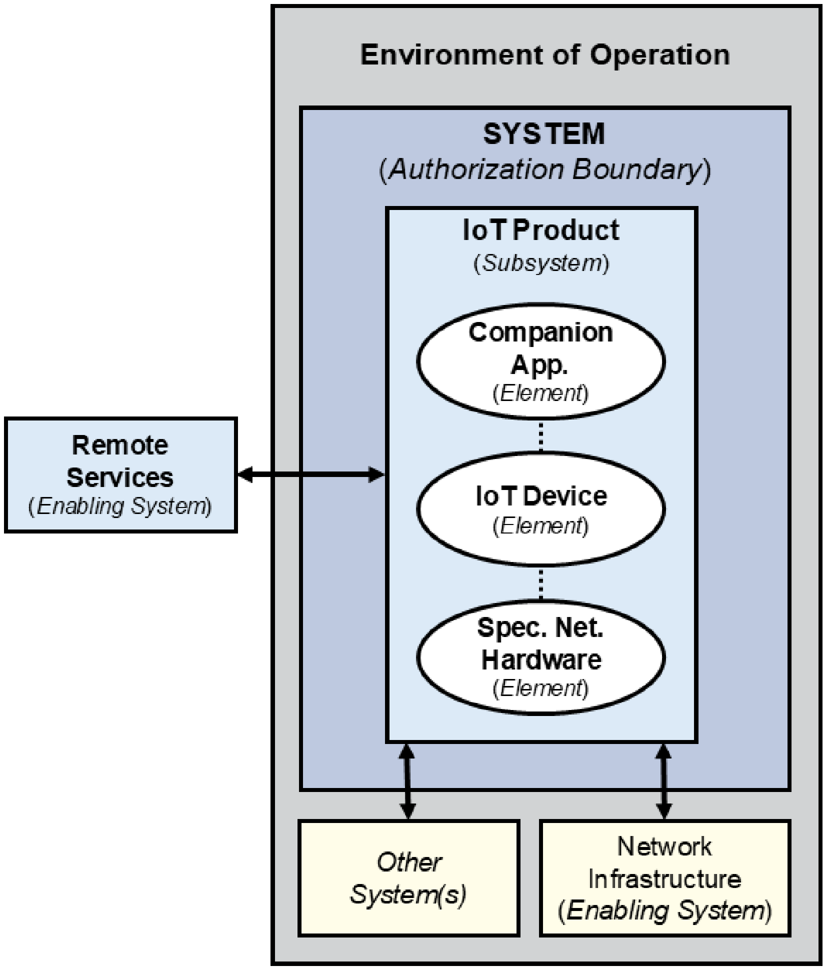

Figure 5 - IoT Product Represented as a Standalone System

Other IoT products acquired by organizations may be best characterized with some or all IoT product components integrated as a subsystem or element of the system defined by the authorization boundary of a larger system. Organizations have flexibility in how they organize system elements and subsystems within their managed authorization boundaries, and they may have several considerations that drive a particular system view. For example, a system may be assembled primarily from IoT products and other solutions implemented by subsystems. Such a system may be best viewed as shown in Figure 6.

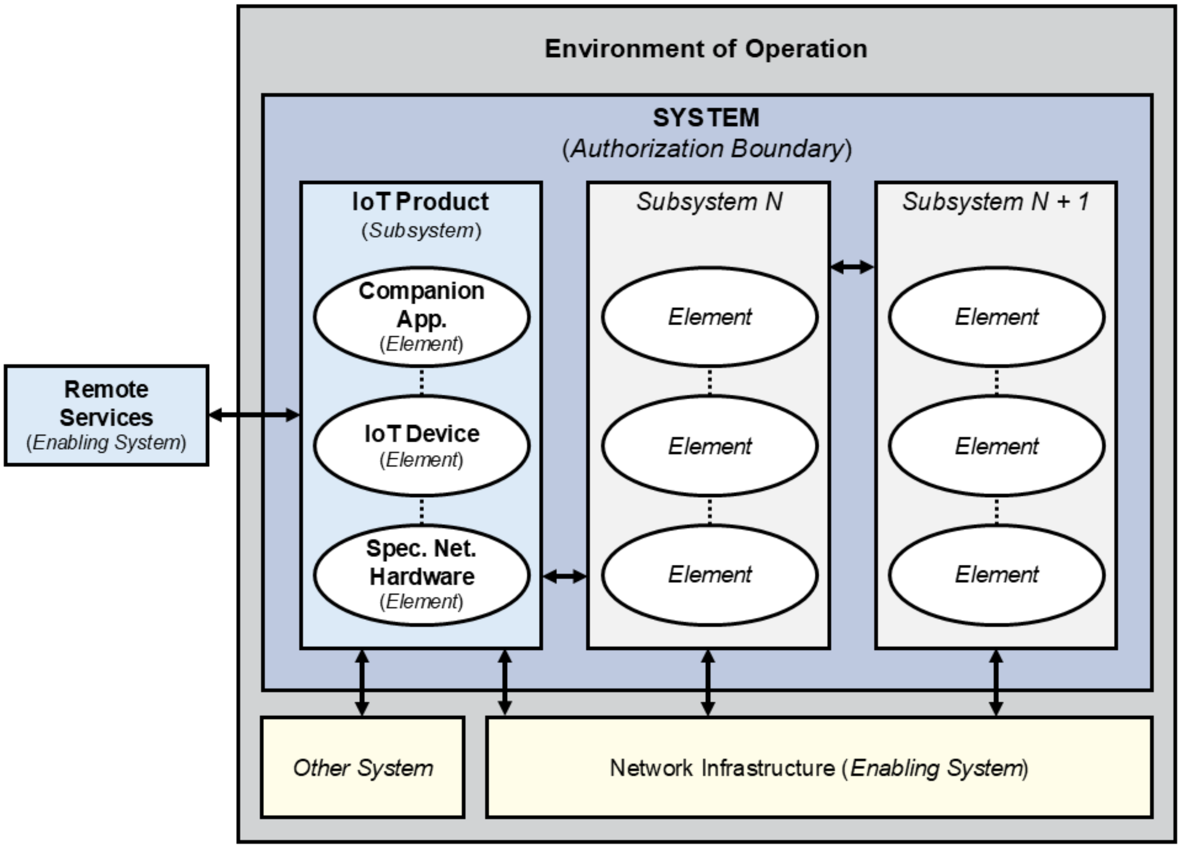

Figure 6 - IoT Product in a System Comprised of Other Subsystems

For other deployments, the locally managed IoT product components (e.g., IoT device, companion applications, specialty networking hardware) may be considered elements of the system, which may be comprised of other elements as well. Figure 7 illustrates this view of an IoT product as part of a system.

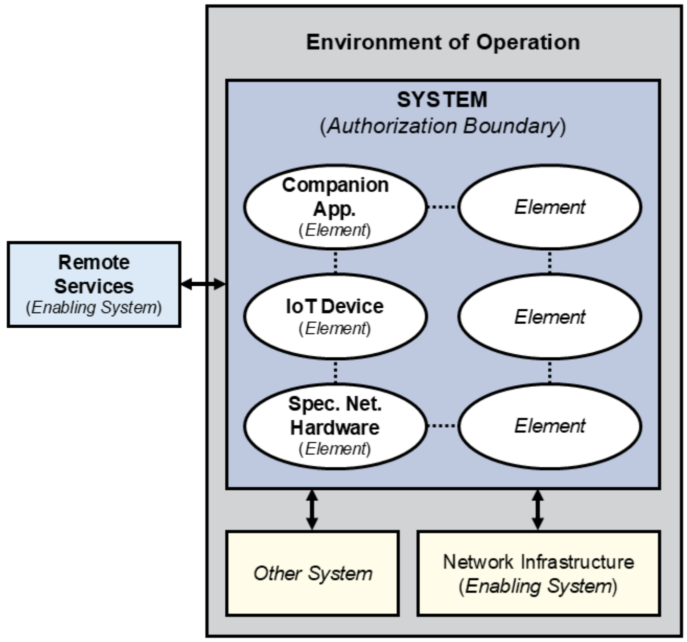

Figure 7 - IoT Product Components Integrated as Elements of a System

In either of the cases depicted in Figure 6 or Figure 7, some IoT product components will fall within an authorization boundary it shares with other system elements. As such, organizations may have significantly more expectations about how this IoT product must support the security controls of the information system and organization due to overall requirements allocation. When security requirements are allocation to IoT products, technical capabilities may be expected from IoT product components to support information system controls; similarly, organizations may depend on non-technical capabilities provided by manufacturers or third parties to support information system controls.

If the IoT product lacks technical or non-technical capabilities to support the information system's security controls, challenges can arise for the organization to manage risk. In this situation, technical or non-technical capabilities lacking in one IoT product component might be provided by other product or system elements or systems (e.g., IoT hub, cloud service, mobile app), or the organization might choose to implement compensating controls (e.g., creating a segmented network for IoT) or reimplement existing controls (e.g., changing a policy or procedure for a control in response to IoT limitations). If risk(s) introduced by the IoT product cannot be mitigated within the organization's risk tolerance level, the organization could accept these new risks or decide not to incorporate the IoT product into the information system.

This publication can apply to IoT products and product components in all scenarios as presented here but is primarily aimed at IoT products where some or all IoT product components are treated as system elements since the organization typically has greater responsibility and control over these types of IoT products. Understanding the relationship of the IoT product and its components to the system is important to properly define the cybersecurity requirements needed to support organizational and system security requirements.

2.3. How IoT Products Support Security

The relationship of an IoT product and its IoT product components to an information system provides context to understand how an IoT product's components support both system and organizational objectives. *Managing Information Security Risk: Organization, Mission, and Information System View,* NIST SP 800-39, [5], discusses how higher-level mission and organizational objectives inform the architecture and control structure around information systems. In this publication, we extend the discussion from [5], highlighting the connection between systems and elements as discussed in SP 800-37 [4] and Sec. 2.1 above. Figure 8 shows the connection between the concepts discussed in [5] and system elements.

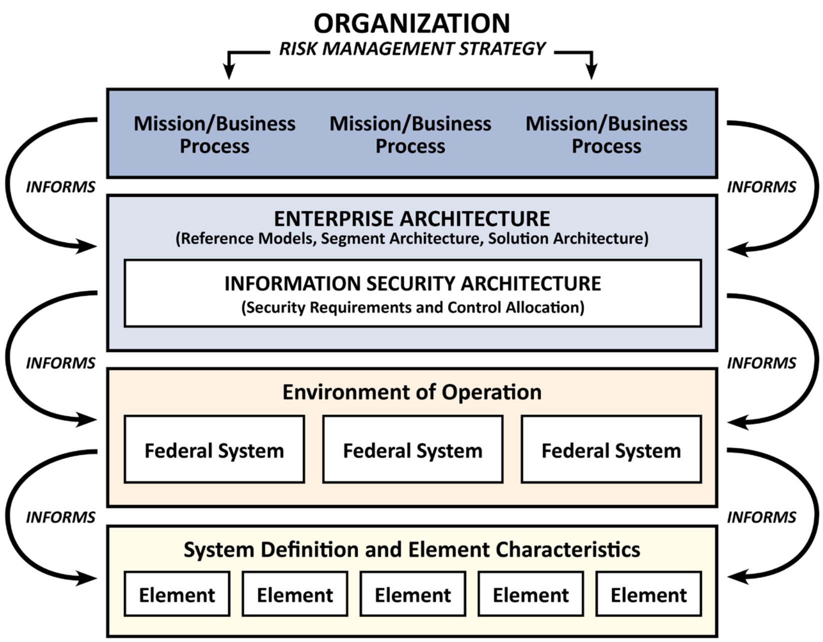

Figure 8 - Information Security Requirements Integration to the Element Level

SP 800-39 [5] describes how the organization's risk management strategy informs the enterprise architecture, including the information security architecture. Key to the information security architecture is the identification of security requirements and the selection and allocation of security controls. Information security architecture informs the federal systems within the environments of operation, particularly through the application of security controls. This publication focuses on IoT products as system elements. When security requirements for the system are therefore allocated to the IoT device and other IoT product components, this implies support for the system and its security controls. We can call these allocated security requirements *IoT product cybersecurity requirements* when identifying them for IoT products.

Consider: How IoT Product Cybersecurity Requirements Can Be Building Blocks for Success

In the context of this document *IoT product cybersecurity requirements* refers to the cybersecurity support necessary from an IoT product to support the deploying organization and systems. IoT product cybersecurity requirements state the *technical* and *non-technical support* needed from an IoT product that will be a system element, system, or subsystem to which security controls will be allocated. Technical support are features or functions implemented using hardware or software, and the technical support allocated to IoT devices or other IoT product components are called *IoT product cybersecurity capabilities*.

Note, there is a reflective relationship, but critical distinction, between system cybersecurity controls and the IoT product cybersecurity capabilities that are needed to support them. IoT product cybersecurity capabilities reflect the technical support needed across a system to support security controls. Therefore, IoT product cybersecurity capabilities may not be unique to the IoT product and could be the same as would be expected from any other system element. For example, an organization may require that data be protected while at-rest, which includes when product data is stored on the IoT device and in a remote service. In this case, both IoT product components should implement strong encryption and data access controls, as would be expected for other system elements or subsystems that the organization can use to meet its requirement to protect data at-rest. The hardware and software along with the resulting features and functions that are used to implement technical cybersecurity capabilities may vary for different IoT product components even if they are supporting the same cybersecurity control. For example, organizations commonly require all software to be kept up to date. For locally managed IoT product components, this may require the organization using the IoT product to perform an action to apply the update, but for remote services, the organization that manages that service will ensure software updates are applied.

In addition to technical means, non-technical support can also be critical in supporting the application of system security controls. Therefore, allocated cybersecurity requirements can also include *non-technical supporting capabilities*, which are actions that manufacturers or third parties take in support of the initial and on-going security of IoT products. Since non-technical supporting capabilities are implemented using procedures and processes rather than hardware and software, non-technical supporting capabilities may be able to be implemented for an IoT product, including all of its product components, with one instantiation.

Details: Example IoT Product and Non-Technical Supporting Capabilities

For an IoT product such as a smart appliance, a cybersecurity capability could be the ability to establish, manage, and enforce authentication and authorization for entities that attempt to access the IoT device, other product components or data that the product produces or transmits. A corresponding non-technical supporting capability could be manufacturer-provided instructions on how authentication and authorization policies can be established and managed in the product.

Both IoT product cybersecurity capabilities and non-technical supporting capabilities are vital to organizations' ability to implement controls that the organization has allocated for their information systems. Figure 9 illustrates how IoT product cybersecurity capabilities and non-technical supporting capabilities (grouped together as 'IoT Product Cybersecurity Requirements') support system/organizational security capabilities, which in turn satisfy organizational security requirements.

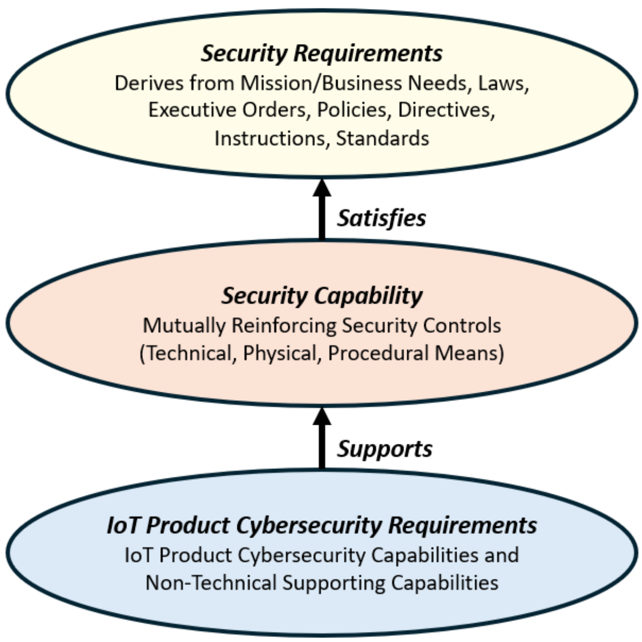

Figure 9 - Role of IoT Product (Technical) Cybersecurity and Non-Technical Supporting Capabilities in Satisfying Security Capabilities and Requirements

Selecting, allocating, and implementing security controls to information systems are key tasks of the RMF Select and Implement Steps. See SP 800-37 [4] for more information and detailed task descriptions of the Select and Implement Steps. Controls used by federal agencies are selected from *Security and Privacy Controls for Information Systems and Organizations,* NIST SP 800-53, Revision 5, [7]. These controls are technology agnostic and can apply to IoT products incorporated into systems as system elements.

For more background on the topic of how IoT products can support cybersecurity, the NISTIR 8259 series discusses the concept of IoT product cybersecurity extensively from the manufacturer's perspective—that is, for manufacturers to understand the capabilities that customers need in IoT devices. But the information in the NISTIR 8259 series could also be helpful for organizations as they acquire and integrate IoT devices.

NISTIR 8259, *Foundational Cybersecurity Activities for IoT Product Manufacturers* [23], while focused on manufacturers, can help organizations consider their needs and goals related to IoT products. In particular, NISTIR 8259 highlights how IoT products will likely be developed with a specific customer and use case as a target. Further, NISTIR 8259 discusses the importance of device cybersecurity capabilities to customers since they help customers help customers in their role as deployer, meet their security requirements. In light of this, NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline* [24] provides a starting point for IoT product cybersecurity capabilities needed by many customers in many IoT use cases to support various cybersecurity risk mitigation goals. Likewise, NISTIR 8259B, *IoT Non-Technical Supporting Capability Core Baseline* [25] is a starting point for non-technical capabilities provided by manufacturers and/or third parties (i.e., supporting entities) that also support customers' cybersecurity risk mitigation goals.

Details: Difference between the IoT Core Baselines and SP 800-53B Control Baselines

Readers may be familiar with the low-, moderate-, and high-impact security control baselines in *Control Baselines for Information Systems and Organizations,* NIST SP 800-53B, [8]. The IoT core baselines are distinct from the SP 800-53B security control baselines. The IoT core baselines define high-level IoT product cybersecurity capabilities and non-technical supporting capabilities, while SP 800-53B security control baselines provide a risk-based starting point for security control selection. The IoT product cybersecurity capabilities and non-technical supporting capabilities presented in the IoT core baselines enable IoT devices to *support* the controls in a SP 800-53B control baseline. SP 800-213A, *IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog* provides more specific capabilities than the IoT core baselines that are targeted at SP 800-53 security controls.

2.4. How IoT Products May Create Security Challenges

Integrating an IoT product into a system can present a number of challenges for organizations. Organizations should strive to understand these challenges before an IoT product is acquired and integrated into a system. Due to a number of market and technological factors, IoT devices or IoT products often lack cybersecurity functionality commonly present in conventional IT equipment (e.g., laptops). For example, an IoT product's remote service may not meet geographic and jurisdictional requirements for an organization seeking to retain control over their data. Support for multi-factor authentication for all IoT product components, particularly IoT devices, may be limited. Some IoT product components may have computing resource constraints that inhibit the adoption of some encryption modules.

An IoT product could introduce unacceptable levels of risk to the system when it lacks particular cybersecurity functionality or support. This cybersecurity functionality or support can be called a *key cybersecurity requirement*. Key cybersecurity requirements are those the organization has determined the IoT product must possess and/or manufacturers and supporting entities must provide for the device to be integrated into the system. Key cybersecurity requirements are important to consider because without them, an IoT product cannot be considered "securable" by the organization and will not be able to be used as intended or possibly at all. If other cybersecurity requirements (i.e., those not considered key) are lacking from the IoT product or manufacturers and supporting entities, other IoT product cybersecurity and/or non-technical supporting capabilities or other security controls entirely could possibly be compensating. This gives organizations options when encountering challenges integrating and using IoT products. Thus, organizations should consider all IoT product cybersecurity requirements needed to support security controls, but also carefully assess which requirements they consider key, ensuring they are limited to those that *must* be supported through the product or by the manufacturer and/or supporting entities.

NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* [22] details some of these challenges that IoT devices can create for organizations. The challenges described in NISTIR 8228 represent generic, high-level use cases. For specific organizations or particular IoT devices and IoT products, the challenges faced could diverge from those explored in NISTIR 8228. Organizations are nonetheless encouraged to apply the concepts in NISTIR 8228 to identify challenges applicable to their use cases.

Details: Overview of NISTIR 8228 Concepts

NISTIR 8228 explores a number of challenges, grouped around conventional risk mitigation areas such as asset management, data protection, incident detection, and vulnerability management. The publication further groups these areas into goals of protecting device security, data security, and/or individual privacy. Challenges can arise that hinder risk mitigations in various areas or could impact some or all of the goals. For example, to mitigate risks related to vulnerability management, software updates may need to be performed. However, not all IoT devices allow for software updates (Challenges 8, 10, and 11). Even mitigations as simple as hiding passwords might not be achievable on IoT devices (Challenge 17).

Organizations should not underestimate the challenges of integrating an IoT product into an information system. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems,* NIST SP 800-160, Volume 1, [15] demonstrates how an integrated process is best for engineering trustworthy systems. SP 800-160 Vol. 1 presents concepts reflected in other NIST SPs from a system engineering perspective, giving a detailed look at how trustworthy systems can be engineered. The approach outlined in SP 800-160 Vol. 1 considers acquisition of elements and other system components earlier in the system design process than integration of these pieces. Adequate acquisition and integration processes are important concepts from SP 800-160 Vol. 1 that can help organizations ensure the trustworthiness of their systems.

Systems will be initially designed and implemented (i.e., prepared, categorized, etc.), but then modified as system elements are removed or other elements added. When an IoT product is added as a system element—typically as a subsystem—organizations should consider how the integration of the IoT product as a subsystem could impact the information system and broader security requirements. However, integrating an IoT product into an information system can also be aided by taking a more focused look at the IoT device. Taking this device-centric perspective, an organization can identify and articulate the IoT product cybersecurity requirements (i.e., the set of IoT product cybersecurity capabilities and non-technical supporting capabilities) required from IoT devices and manufacturers/third parties to support security capabilities and satisfy security requirements as well as the overall product cybersecurity requirements. Organizations should be aware that even if the allocated IoT product cybersecurity requirements are provided by a device and manufacturer/third party, the integration of the IoT device into an information system can still introduce risk.

3. Identifying IoT Product Cybersecurity Requirements for IoT Products

This section provides organizations guidelines for determining the applicable cybersecurity requirements (i.e., the set of cybersecurity capabilities and non-technical supporting capabilities) needed to secure the IoT product and support system security controls. The high-level process is shown in Figure 10.

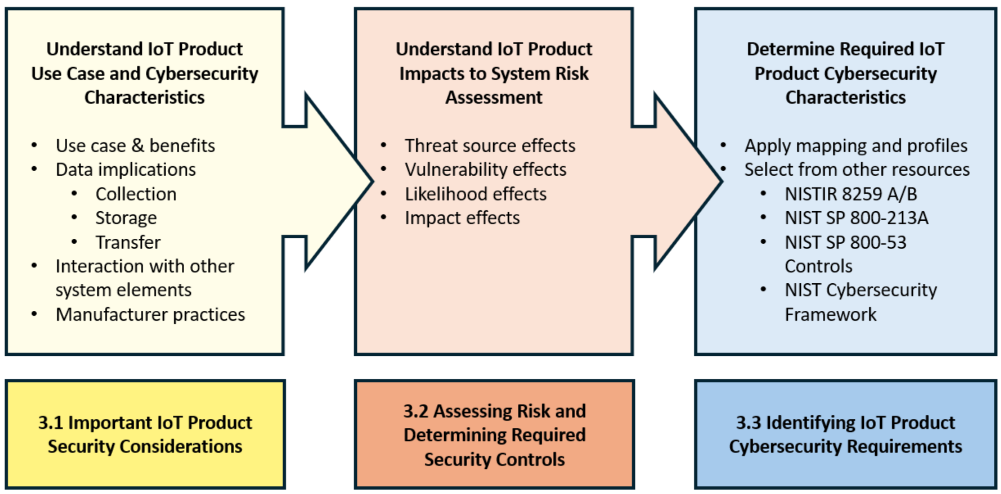

Figure 10 - Organizations Can Use this Section to Identify IoT Product Cybersecurity Requirements

Section 3.1 provides an overview of important IoT cybersecurity considerations. The questions in section 3.1 help organizations contemplate the IoT use case, providing a foundational understanding of how the IoT product might impact risk to the system. Section 3.2 discusses how an understanding of the IoT use case can impact the system's risk assessment and the subsequent allocation of security controls to the information system. Section 3.3 focuses on determining applicable IoT product cybersecurity requirements based on the risk assessment and controls allocation from Section 3.2. The section presents sources of IoT product cybersecurity requirements. Organizations may reference these sources when selecting applicable IoT product cybersecurity requirements.

Each organization should develop a process for identifying and articulating IoT cybersecurity requirements that aligns with their existing policies and procedures (e.g., acquisitions, security, system administration).

Consider: Coordinate Early Within the Organization to Acquire IoT Products

Readers should be aware that even once IoT product cybersecurity requirements are identified and a suitable IoT product is found on the market, procurement challenges may arise. Some organizations maintain exclusion lists that prohibit the procurement of commercially-available products based on country of origin or other criteria. For that reason, it is advisable to begin communicating as early as possible with applicable organizational personnel to navigate through any organizational restrictions.

The guidelines presented in this publication provide a starting point for organizations—as well as additional resources organizations can use—in identifying IoT cybersecurity requirements. The steps described in this section happen before an IoT product is purchased and/or integrated. At this stage, the IoT product itself may not be in the organization's possession, which may result in some considerations, particularly those related to *how* risks can be mitigated, not being entirely known. Information about additional IoT product and support limitations should be identified through further engagement with the available manufacturers and vendors.

3.1. IoT Cybersecurity Considerations

There are many reasons to integrate an IoT product into a system (e.g., to achieve business objectives, further technical advancements, provide administrative support). The reason the IoT product is being acquired will determine its use case. For one organization, IoT sensors may be sought to help remotely monitor environmental conditions; another organization may acquire IoT office equipment to increase productivity; still other organizations may seek to leverage IoT technology in the delivery of services to citizens.

Organizations should fully understand the specific use case for an IoT product since the use case could impact risk to the system and organization. The following questions can help organizations think through some of the common considerations for acquiring IoT products, but this list is not exhaustive. The answers to these and other questions can ultimately help organizations assess risk and identify IoT cybersecurity requirements for their use case(s). Accurately and completely answering these questions for many IoT products will require consultation with IT personnel within the organization.

1. **Are there commercially available products that meet the use case for the IoT product or will the IoT product be custom or customized using other components?** Before a product can be integrated into a system, it must exist – leading organizations to the question of "build or buy?". That is, the product must be created internally or acquired from a third party. The build-or-buy decision is a governance matter, not simply a technology or procurement choice, because it drives distinct cybersecurity considerations, controls responsibilities, and risk management approaches. Products that are built internally and those acquired from third parties carry different risk profiles, and require different stakeholder involvement (e.g., procurement, engineering, legal, compliance, leadership). Notably, the decision typically needs to be made upstream of integration, as the engineering vs. sourcing needed to enable the device precedes its integration. As such, the build-or-buy decision should be addressed as an early, cross-stakeholder governance decision with executive visibility into why the decisions were made.

    2. **What is the expected benefit of the IoT product and how will it be used?** Organizations can help ensure that cybersecurity requirements receive proper consideration by establishing the benefit(s) explicitly for integrating the IoT product and understanding how it will be used. For example, if the IoT product is replacing equipment that did not previously connect to the system, organizations should holistically consider the benefit

of the connection to the system compared to the potential risks. It may be the case that a connected motion sensor can detect potential intruders but may also introduce security vulnerabilities that may outweigh the proposed benefits.

3. **What data is collected?** IoT products can collect many kinds of data, some innocuous, others of concern to organizations. Any data collected could be a risk to the organization. All data collected or reported by the IoT product should be understood, but three main types of data may be of concern:

    a. *Personal data:* Many IoT products can sense or collect data of, from, or about people, which can constitute personal data and represent privacy sensitive data (e.g., Personally Identifiable Information).

    b. *Confidential organizational/Federal government data:* The IoT product may collect restricted or confidential data (e.g., Controlled Unclassified Information, Intellectual Property), which could influence its risk level. For example, IoT products may help create or have access to organization-restricted test results, analysis materials, or device prototypes that require special protection.

    c. *Environmental data:* Many IoT products can sense and/or collect data of, from, or about the physical environment. Organizations should consider whether the collection of environmental data poses any risk to individuals or the organizational mission.

4. **In what technologies will the data be stored and how will it be transmitted?** Many IoT products rely on connections to cloud services and mobile/web applications. These are part of their architecture and central to the product's functionality. IoT products can also connect to additional external services, which may be provided and hosted by a number of third parties, across a range of platforms. Organizations should consider where the IoT product might store data —in the device, the manufacturer's network, a manufacturer-contracted entity's network (e.g., cloud service provider[2]), etc. Cloud services are increasingly used as part of the core IoT product's functionality, enabling authentication, managing updates, storing telemetry, and data transit. Organizations should also consider how the data will be secured in transit as connections to external services and third parties are made and used. Further, products supporting federal systems are subject to FedRAMP requirements as part of the acquisition process.

5. **In what geographic areas will the data be shared or stored?** The architecture that supports IoT products is increasingly global. Organizations should consider where data from prospective IoT products will be transmitted and stored to ensure applicable

[2] As a reminder, if an IoT device uses cloud computing technologies, organizations need to refer to NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing* [13] for additional information on cloud security considerations, as well as SPs 800-145, *The NIST Definition of Cloud Computing* [14] and 800-146, *Cloud Computing Synopsis and Recommendations* [31] for additional information on cloud computing and storage technologies. Finally, NIST SP 500-292, *NIST Cloud Computing Reference Architecture* [1] may be a useful additional resource for organizations.

security requirements are met. An IoT product may connect to and transmit data to systems in many diverse areas, including other cities, states, and countries. These connections may change over time due to the dynamic nature of IoT systems.

6. **With what other third parties will data from, or about, the IoT products be shared or stored?** In some product architectures, an IoT product will only exchange data with the owner and manufacturer-owned and operated systems. In other instances, the IoT product will share data with third parties. For example, many manufacturers use cloud storage and services from other providers to support their IoT products' backend infrastructure.

After understanding the contextual and structural considerations about the IoT product discussed above, organizations should consider the following questions about how the IoT product will interact with the organization and information system:

1. **Might the product interfere with other aspects of operations or system functionality?** Unlike conventional IT equipment, IoT products are more likely to interact with the physical world through sensing and/or actuating. This interaction increases the possibility that an IoT product could affect the organization's operations and the environment (e.g., alarms, thermostats, environmental controls, heating elements) as well as the security posture of the system. For example:
    a. *Could the IoT product introduce privacy or safety risks for people?* IoT products could collect and share sensitive data about people, including, but not limited to, audio and video data. An IoT product can also interact with the physical world (e.g., IoT vehicle) or might be intended to protect human safety (e.g., an IoT smoke alarm), potentially posing safety risks. Considering if an IoT product may introduce privacy or safety risks is critical to planning for risk mitigation.

    b. *Could the IoT product interfere with system reliability or resiliency?* The diversity of IoT product use cases also creates the possibility that the IoT product's expected operational environment may vary from where it is actually deployed. In such an instance, the IoT product might negatively interact with other system elements or operational systems if not properly planned for. For example, an IoT device may go offline to apply a software update. This behavior is acceptable in many circumstances but may impact system reliability if the offline device hurts operations in other parts of the system. Likewise, IoT product components may not be as digitally and physically resilient as their IT or OT counterparts since IoT products must sometimes attempt to deliver both IT and OT functionality. This can lead to inherent practicality and cost constraints that result in a focus or prioritization of some features or aspects of functionality over others (e.g., safety over cybersecurity) in the design of the IoT product.

2. **Would the IoT product introduce unacceptable risks to the organization or result in non-compliance with cybersecurity requirements?** Some IoT products might be unable to support the organization's current security controls as they are implemented due to

their design, requiring organizations to implement compensating controls (e.g., additional organizational controls or alternative technical controls) to manage risk. Organizations should consider the proposed IoT product use case and whether the risk introduced is acceptable. In some use cases, the IoT product might provide an additional point of access to the system from which an attacker could pivot to other system elements or networks.

3. **Does the IoT product have known security and/or privacy vulnerabilities?** Like all connected products, IoT products attract attention from security professionals and researchers who identify security and/or privacy concerns. Manufacturers also commonly publish similar information concerning their products. Understanding known vulnerabilities can inform an organization's acquisition, risk assessment, and possible integration of an IoT product. For example, if known vulnerabilities exist that the manufacturer cannot mitigate, organizations would have to identify and address risks introduced by the IoT product through other means.

As discussed extensively in NISTIR 8228 [22], IoT devices can have significantly different feature sets compared to conventional IT devices. These differences in device capabilities and support for security controls can create challenges for organizations if not adequately planned for, especially if the capabilities diverge significantly from what is expected. Organizations should refer to NISTIR 8228 and consider if the IoT product will create any security and privacy challenges for the information system and organization. One common way challenges arise is when an IoT product does not fully support *key cybersecurity requirements*. For example, a pillar of Zero Trust Architectures is that devices (of all kinds) are secure and comply with policy, which includes limitation of access in line with zero trust principles [32]. Thus, support for zero trust principles could be considered part of an IoT product's key cybersecurity requirements if it will access systems that implement a zero-trust architecture.

Organizations may reduce these challenges by considering important aspects of how the IoT product should connect and function to ensure the product conforms with expectations, and thus, may define, inform, or otherwise impact key IoT product cybersecurity requirements. In particular, organizations should consider:

1. **What organization-specific considerations are important to defining key cybersecurity requirements?** Organizations often invest in specific solutions or implementations that would be the preferred support for various security controls. Identifying these kinds of organizational considerations can help guide a purchase and reduce conflicts in applying security controls if the IoT product is integrated into an existing organization system. Since IoT products can interact with an organization in many ways (e.g., via the network, but also in a physical way), many different kinds of organization-specific considerations can impact what is acceptable to an organization, which mitigations are practical and appropriate, and the determination of cybersecurity requirements. Some examples of organization-specific considerations include, but are not limited to:
    1. *Does the organization require Personal Identity Verification (PIV) card-based authentication or does it allow another form of multi-factor authentication in limited circumstances?* Support for critical cybersecurity technologies and operations that

are used to implement security controls may be important for an organization in deciding which, if any, IoT product to use for a particular purpose. Organizations should note that some of this support, such as support for PIV may be related to standards and guidelines like the Federal Information Processing Standards (FIPS)[3].

2. *Does the organization purchase products from particular manufacturers or 3rd parties?* Such situations may limit the IoT products readily available to the organization. This may, in turn, limit availability of IoT products that best support the needs and goals of the organization.
3. *Are there any environmental considerations (e.g., exposure to the elements, human presence, sensitive data that could be collected) in the environment of operation?* Environmental considerations can help guide cybersecurity requirements, particularly around physical protections. For example, if an IoT device is meant to be placed outdoors, a durable housing may be needed to withstand excessive heat, cold, and moisture while still providing data availability and integrity.

2. **Does the IoT product lack key cybersecurity requirements?** Key cybersecurity requirements are those the organization has determined that the IoT product must possess for the product to be integrated in the system and make external connections to other systems or the Internet. For the IoT product, lack of key cybersecurity requirements indicates that the IoT product may not support existing information system controls, which subsequently introduces unacceptable levels of risk. To support information system security controls, the organization may need to consider if other product components (e.g., a gateway, hub, cloud service) or system elements can provide the capabilities missing from the IoT device but should keep in mind those *key cybersecurity requirements* that cannot be provided elsewhere, otherwise compensated for, or omitted without introducing unacceptable risk to the organization.

Consider: Risk Appetite

Since key cybersecurity requirements are tied to a "unacceptable" level of risk when omitted, their identification will be related to both the IoT device and its use case, but also the organization and, among other considerations, its risk appetite (i.e., the types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value [26]). A higher risk appetite when using the IoT device may lead to fewer key cybersecurity requirements since, at a minimum the organization is more willing to omit support for a security control despite the risk it introduces. An organization with a lower risk appetite may be less willing to accept risks left unmitigated by the lack of IoT product cybersecurity requirements and thus not willing to omit the requirement if lacking from an IoT device. Proper understanding of risk

[3] NIST's current FIPS can be found at https://www.nist.gov/itl/current-fips. Relatedly, organizations should be aware of the Cryptographic Module Validation Program (CMVP) when considering appropriate cryptographic modules for IoT devices. More information about the CMVP can be found on the project webpage at https://csrc.nist.gov/projects/cryptographic-module-validation-program.

appetite and other cybersecurity considerations will require input from IT security personnel.

3. **Will the implementation or mismatched maturity of cybersecurity capabilities and/or non-technical supporting capabilities fail to satisfy key cybersecurity requirements?** Some IoT products may completely lack key cybersecurity requirements, and other IoT product components cannot supply the capabilities, potentially making the IoT product unusable by the organization. Other IoT products may provide cybersecurity requirements but not in the manner expected by the organization. For example, an IoT device may have a unique device identifier, but it may not be in a format the organization uses with other equipment. The organization will need to plan for how this identifier will be incorporated into its asset management processes. When an IoT product's cybersecurity capabilities lack appropriate maturity, the task of securing the product may be much more difficult. For example, an IoT device may encrypt data, but use a deprecated encryption module due to device resource constraints. In this case, the organization may need to apply significant compensating controls.
4. **What are the physical, logical access, network, and other requirements of the IoT product and how do they relate to key cybersecurity requirements?** An understanding of how the IoT product will interact with the digital and physical worlds is important to understanding whether the product should be used by the organization and, if so, the cybersecurity risks and corresponding mitigations that are practical, possible, and appropriate. For example, knowing the endpoints (both internet domains and local devices) the IoT product must connect to can help an organization ensure all connections the product will make (and the logical access via those endpoints) are acceptable within the organization's security policy. Physical requirements, such as the need to access the IoT device component for maintenance or diagnostics may conflict with how some products are deployed (e.g., if they must be placed in an inaccessible location making physical maintenance difficult or impossible).
5. **Are there applicable product cybersecurity transparency mechanisms that demonstrate that the IoT product meets one or more key cybersecurity requirements?** The heterogenous IoT product marketplace has prompted the development and deployment of various cybersecurity transparency mechanisms for IoT products or IoT product components. For example, the United States Government's Cyber Trust Mark (CTM) as well as programs operated by other nations and the private sector can provide organizations with insights into the cybersecurity of IoT products. Other programs that may relate to specific IoT product components, such as cloud certification programs can provide similar insights to organizations related to these components if communicated. Organizations should carefully understand and consider the structure, requirements, outcomes, etc. of any transparency mechanisms since all these factors can vary and have implications for how these mechanisms may demonstrate that the IoT product has one or more key cybersecurity requirements.

In addition to the specifics of the IoT product and how it works, organizations should also consider the practices of the manufacturer in the development and on-going support of the IoT product. Secure development, supply chain, and maintenance (e.g., vulnerability management and patching) practices can help mitigate the introduction of vulnerabilities and possibly reduce likelihood and/or impact of adverse events. Consider:

1. **Does the manufacturer use secure development and supply chain practices to support their operations?** The use of secure development and secure supply chain practices in the manufacture of IoT products will not solve all cybersecurity issues but will help reduce cybersecurity issues with IoT products and provide additional assurances to organizations of the cybersecurity posture of the manufacturer and IoT product. Additional information on secure development as it relates to software can be found in NIST's *Secure Software Development Framework* (SSDF) [30]. More guidelines for organizations in "identifying, assessing, selecting, and implementing risk management processes and mitigating controls throughout their organizations to help manage information and communication technology (ICT) supply chain risks" can be found in *Supply Chain Risk Management Practices for Federal Information Systems and Organizations,* SP 800-161 [17].

2. **How robust and mature are the manufacturer's vulnerability disclosure and remediation practices?** Organizations should consider whether the manufacturer has an established vulnerability disclosure program with a history of timely updates and should look to these disclosures to inform themselves of known vulnerabilities.

3. **What are the expectations around delivery of software updates in response to discovered vulnerabilities?** Since removal of vulnerabilities is important to maintaining an organization's risk posture, understanding expectations around update delivery can avoid the introduction and exploitation of vulnerabilities by allowing organizations to adequately plan for the delivery (or absence) of an update to apply.

4. **How are risks to product availability due to physical failure or degradation mitigated?** Availability of the system that incorporates the IoT product will partially depend on maintaining the availability of that product. Product availability may rely on the ability to repair or replace physical IoT product components. Thus, organizations should plan for the availability (or absence) of replacement product components or parts. IoT products that perform mission-critical functions and are deployed in harsh physical conditions may have more stringent repair and maintenance needs. For example, a sensor placed in a damp location may face the potential of the product's availability being put at risk by physical failure of the IoT device housing and internal electronics. If this sensor provides mission-critical data, this risk could mean potentially high enough impacts to warrant one or more mitigations including, but not limited to ensuring a supply of replacements and parts.

The questions in this section assist organizations in understanding key aspects of the use case of the proposed IoT product as well as the risk that could be introduced by incorporating it into an existing system. The list of questions is not exhaustive.

3.2. Assessing Risk and Determining Required Security Controls

Organizations should remember that the incorporation of an IoT product can alter the information system's risk assessment. Any change in the risk assessment may require the allocation of additional security controls or the introduction of compensating controls to reduce risk to acceptable levels. Section 3.1 provides a starting point for considerations about IoT products that may help organizations determine the risk associated with an IoT product. Organizations assess risk to and from IoT products using the organization-defined approach based on guidelines in NIST SP 800-30 [3] but supplement the risk model for IoT using the guidelines in this section.

Figure 11 illustrates how to update a risk model specifically for an IoT product, closely aligned and adapted from the risk model with key risk factors identified in SP 800-30 Rev. 1 [3]. This updated risk model would then be used with other information to assess risk to the system, including the IoT product as an element.

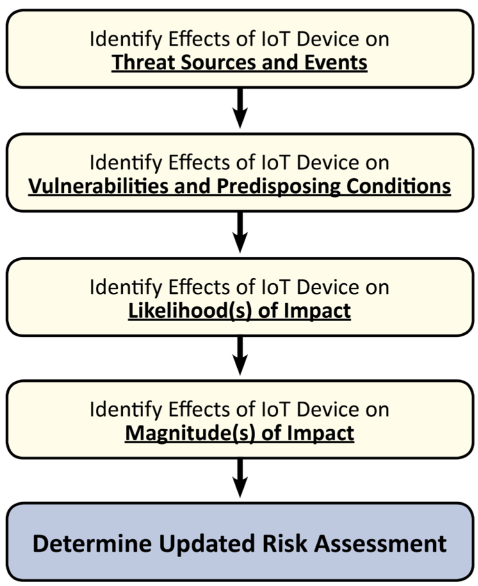

Figure 11 - Steps to Updating a Risk Model and Risk Assessment using New Information about an IoT Product

Ideally the inclusion of an IoT product as a new system element will not significantly alter the information system's risk assessment. Nevertheless, as part of the risk management process, organizations must assess the level of risk introduced by the IoT product. The following discussion of threats, vulnerabilities, likelihood, and impact shall be considered by an organization as part of the risk model of an IoT product to be incorporated into a system and the subsequent updated risk assessment of the system.

3.2.1. Effects on Threat Sources and Events

How does the IoT products affect the threat sources and events that must be considered as part of a risk assessment? An IoT product may bring new features and functions to a system but may also attract new threat sources (i.e., situation, intent, or method that may trigger a vulnerability) and present new threat events (i.e., observable occurrences within the system that causes undesirable consequences or impacts) that must be considered as part of a system risk assessment. For example, IoT products may introduce new safety- and/or mission-critical considerations to a system. These considerations could make the system more attractive to attacks that previously would not apply (e.g., the system may become a ransomware target) and/or create events not previously possible (e.g., people put in physical danger). Conversely, IoT products may also not face the same threat sources and events that the rest of a system might. For example, IoT products with a short lifespan, limited functionality, or limited accessibility may not be subject to some threat sources (e.g., attackers aiming to do medium- to long-term reconnaissance) or some events (e.g., those that require extended, consistent network access). IoT products will often have many of the same threat sources and events as the existing information system. There may be a set of unique IoT product threat sources and events as well as some information system threat sources and events that do not apply to the IoT product.

In this sense, there are two classes when comparing threat sources and events between the IoT product and information system: the threat sources and events can be the ***same*** or ***different***. *Same* means the sets are identical such that the IoT product brings no new threat sources or events but faces all the same threat sources and events as previously considered in the system's risk assessment. *Different* sets can be one of several categories:

1. No previously considered threat sources and events apply, only new threat sources and events (may) apply.
2. Some, but not all, previously considered threat sources and events apply, and new threat sources and events apply.
3. Some, but not all, previously considered threat sources and events apply, but no new threat sources and events apply.
4. All previously considered threat sources and events still apply, and new threat sources and events apply.

3.2.2. Effects on Vulnerabilities and Predisposing Conditions

How does the IoT product affect vulnerabilities and predisposing conditions considered as part of a risk assessment? As defined in Committee on National Security Systems Instructions (CNSSI) No. 4009, "a vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source." [19] Additionally, predisposing conditions are characteristics of the environment, organization, or system that contribute to the likelihood that once initiated, threat events will result in undesirable consequences or impacts. An updated list of threat sources and events may help organizations identify vulnerabilities and predisposing conditions not previously considered as part of the risk assessment. These vulnerabilities could reside in the information system or in the proposed IoT product. Alternatively, considering potential vulnerabilities in an IoT product (e.g., default credentials that cannot be changed) may help the organization identify additional threat sources (e.g., credential stuffing authentication attack). For example, a minimal threat of system elements being compromised and assimilated into a Distributed Denial of Service (DDoS) -executing botnet may have existed before, but a proposed IoT product deployment within the system may introduce vulnerabilities (e.g., default credentials) and predisposing conditions for this threat to exploit. IoT products may have many of the same vulnerabilities as the existing information system. There may be a set of unique IoT product vulnerabilities as well as some information system vulnerabilities that do not apply to the IoT product.

In this sense, there are two classes when comparing vulnerabilities and predisposing conditions between the IoT product and information system: they can be the <u>*same*</u> or <u>*different*</u>. *Same* means the sets are identical such that the IoT product brings no new vulnerabilities or predisposing conditions but has all the same vulnerabilities and predisposing conditions as previously considered in the system's risk assessment. *Different* sets can be one of several categories:

1. No previously identified vulnerabilities and predisposing conditions apply, only new vulnerabilities and predisposing conditions (may) apply.
2. Some, but not all previously considered vulnerabilities and predisposing conditions apply, and new vulnerabilities and predisposing conditions apply.
3. Some, but not all previously considered vulnerabilities and predisposing conditions apply, but no new vulnerabilities and predisposing conditions apply.
4. All previously considered vulnerabilities and predisposing conditions still apply, and new vulnerabilities and predisposing conditions apply.

3.2.3. Effects on Likelihood(s) of Occurrence of Threats

How does the IoT product affect <u>likelihood(s) of occurrence</u> determinations as part of a risk assessment? Risk impact is dependent on two components: likelihood of occurrence and magnitude of impact. As per CNSSI No. 4009, likelihood of occurrence "is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities)." [19] Determination of likelihood as part of a risk assessment is therefore based on identified threat sources and events as well as vulnerabilities and pre-disposing conditions. Threat sources, events, and vulnerabilities identified for the IoT product must be used in the assessment of likelihood. Likelihood of occurrence can often be expressed in a relative way (e.g., low, medium, or high likelihood of occurrence). As part of a risk assessment, the effect of an IoT product on likelihood of occurrence can be expressed as being *greater*, *lower*, or *equal* to the likelihood of occurrence without the IoT product.

For example, an IoT product being connected to a system may create new possible connections (e.g., cellular data connections) that may increase the likelihood of a remote actor being able to exploit a vulnerability. In this case, the system with the IoT product can be said to have *greater* likelihood of occurrence compared to the system without the IoT product. Conversely, an IoT product with limited direct network connectivity (e.g., the IoT device can only communicate with the network through a hub/gateway) may reduce the comparative likelihood that a remote actor can exploit a vulnerability, resulting in a *lower* likelihood of occurrence *for that product*. In some instances of threats and vulnerabilities, the designation of a lower likelihood of occurrence may apply only to the IoT product, not the larger system. This is an important distinction. The system may still face the same overall level of likelihood of occurrence for a threat based on many factors, even if the likelihood of occurrence for the proposed IoT product is lower.

A risk assessment must be performed at the system level, which will help identify security controls appropriate for that system. This publication supports this task through guidelines that help identify cybersecurity requirements for an IoT product that will be connected to another system. This connection between IoT product and organization's system can impact the system's security controls, but consideration of the IoT product does not solely dictate which controls are appropriate for the system. This must consider all elements of the system, connections to other and supporting systems, etc. For example, a system may be comprised of laptops, smartphones, routers and other IT equipment that facilitates the use of cloud services and other external resources. These parts of the system will require a number of security controls to protect the system and its operation. As an IoT product is added to this system, it may operate and function in ways no other system element does, which could change which security controls apply. If the IoT product doesn't store any data, it may not need to meet some data at rest requirements needed on other system elements. The IoT product will still connect to the rest of the system, though, and may need to support other security controls such as protection of data in transit.

3.2.4. Effects on Magnitude(s) of Impact of Threats

How does the IoT product affect <u>magnitude(s) of impact</u> considered as part of a risk assessment? In addition to likelihood of occurrence, a risk assessment will consider the magnitude of impact. Magnitude of impact is defined in CNSSI No. 4009 as the level of harm "that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability." [19] The introduction of IoT products into an information system can expand the harm to include human safety, environmental, and other impacts. IoT products may introduce *greater*, *lower*, or *equal* magnitude of impact compared to the rest of the system. For example, an IoT product that is safety- and/or mission-critical may create *greater* magnitude of impact if compromised. A constrained IoT product (e.g., with limited storage, memory, or processing power), may contribute *lower* magnitude of impact relative to other elements in the system.

3.2.5. Determine Updated Risk Assessment

With an understanding of the threat sources and vulnerabilities introduced by the IoT product, as well as the resulting likelihood of occurrence and magnitude of impact, organizations can perform an updated risk assessment of the information system using information available about the proposed IoT product. Figure 12 shows how information about an IoT product will flow into the updated risk assessment of the system with which the IoT product is integrated. The resulting updated risk assessment may require the organization to allocate new security controls to the information system to effectively manage the anticipated risk. The organization may identify certain security controls that apply to the IoT product, or that must be provided by the IoT product specifically. Ultimately, it is important for organizations to identify all security controls required to reduce information system risk to an acceptable level. Section 3.3 will focus on using the identified security controls to determine the technical and non-technical capabilities needed from the IoT product and/or other system elements.

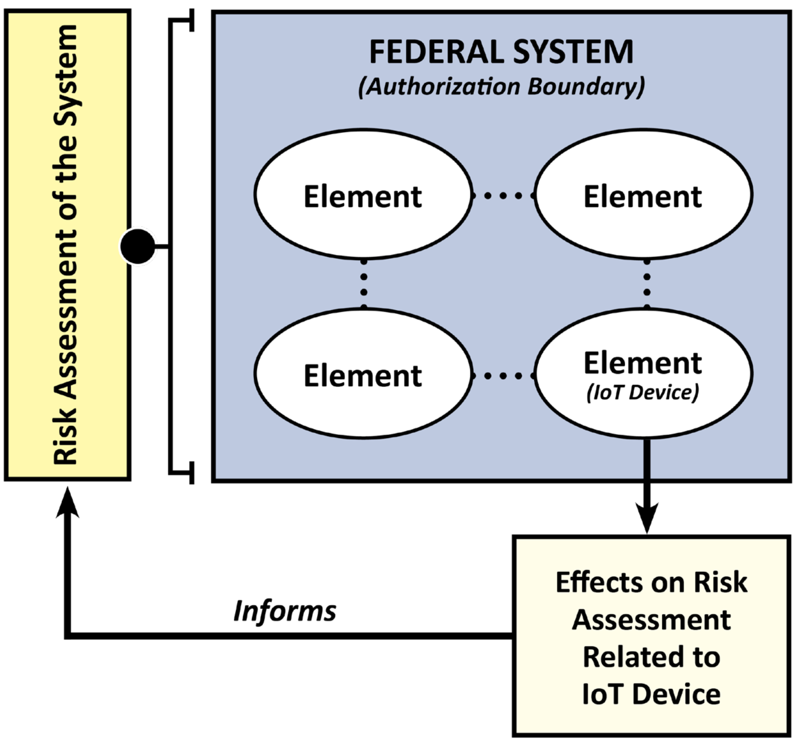

Figure 12: Effects on Risk Assessment due to IoT Product Informs the Risk Assessment of the Entire System.

3.3. Identifying IoT Product Cybersecurity Requirements

IoT product cybersecurity requirements should be based on the security capabilities and security requirements of the system and organization while also accounting for considerations like those highlighted in Sec. 3.1 and updates to the system risk assessment that may be necessary as discussed in Sec. 3.2. Figure 13 illustrates this process and how it will draw on the considerations and guidelines from the prior sections to inform the IoT product cybersecurity requirements.

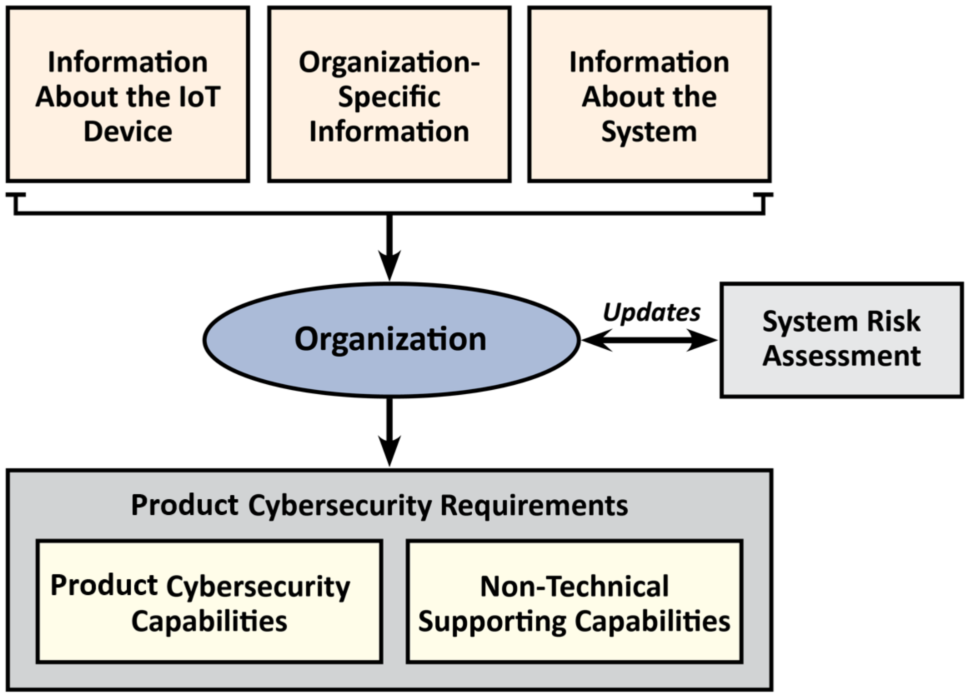

Figure 13: Organizations Can Gather Information to Update the System Risk Assessment and Determine IoT Product Cybersecurity Requirements

Determining IoT product cybersecurity requirements may be challenging for some use cases. To assist organizations in selecting IoT product cybersecurity requirements, this section presents several NIST publications and resources. When the full set of security controls for the system has been identified, organizations can translate those controls into IoT product cybersecurity capabilities and non-technical supporting capabilities. Since IoT product cybersecurity requirements are in support of security controls allocated to information systems, organizations can identify the IoT product cybersecurity requirements needed to support the security controls allocated to the information system(s) to which the IoT product will be connected. Information security and systems administration personnel should collaborate to identify security controls that require support from system elements (e.g., IoT products).

Details: Example of IoT Product Cybersecurity Requirements Supporting Security Controls

An organization might want to acquire an IoT product such as a *smart speaker* to use in the office environment. The smart speaker will need to connect to the system (e.g., internal network) so that organization management can access the speaker from other parts of the environment of operation and play audio over the speaker. These remote connections will require proper authentication and authorization. To support the authentication and authorization controls, the smart speaker may require IoT product cybersecurity capabilities such as the ability to deny remote connections; the ability to authenticate and/or authorize entities attempting to make remote connections; and the ability to terminate connections within organizational policy. Other IoT product cybersecurity capabilities may apply, but these are presented as example capabilities. Additionally, the allocated security controls may require the organization to configure the smart speaker to authenticate and authorize users within organizational policy, which could require non-technical supporting capabilities from manufacturers. These non-technical supporting capabilities could include obtaining documentation from the manufacturer about how the IoT product can be configured to support organizational authentication and authorization policy.

3.3.1. Identifying Requirements using SP 800-213A

Organizations may leverage SP 800-213A of this publication, *The IoT Device Cybersecurity Requirement Catalog* [18]. This catalog contains IoT product cybersecurity requirements organized by technical and non-technical. The IoT product cybersecurity requirements in the catalog are derived from security controls in SP 800-53 [7] and therefore may be helpful in supporting security controls in low, moderate, and high impact information systems. The IoT product cybersecurity requirements (i.e., IoT product cybersecurity capabilities and non-technical supporting capabilities) included in the SP 800-213A catalog were based on the IoT core baselines but adapted the content of those high-level sets of capabilities into more thorough articulations. This adaptation was guided by the SP 800-53 security controls, with the more specific and additional content (relative to the IoT core baselines) developed to support the statements in applicable SP 800-53 security controls and enhancements. Additional information is included in SP 800-213A. SP 800-213A can be a valuable resource for organizations when identifying applicable IoT product cybersecurity requirements.

Organizations can use the mappings (i.e., between SP 800-53 Rev. 5 security controls and IoT product cybersecurity requirements) included in SP 800-213A to identify appropriate IoT product cybersecurity requirements. The mappings show, for each identified SP 800-53 Rev. 5 security control, the corresponding IoT product cybersecurity capabilities and non-technical supporting capabilities needed to support the security control. Using the mapping, the organization will be able to develop a comprehensive list of IoT product cybersecurity capabilities and non-technical supporting capabilities. This list of IoT product cybersecurity capabilities and non-technical supporting capabilities may need to be tailored—just like an organization tailors the SP 800-53 Rev. 5 security controls.

Some IoT product cybersecurity capabilities and non-technical supporting capabilities identified through the mapping may not be applicable to the use case. For example, a required SP 800-53 Rev. 5 security control might map to the capability “Ability to create an organizationally-defined system use notification message or banner to be displayed on the IoT device.” For many IoT products and/or use cases, this capability is not applicable; organizations might choose to scope this identified capability out of the needed capabilities. Other identified IoT product cybersecurity capabilities and non-technical supporting capabilities might be best provided by a different system element (e.g., gateway, IoT Platform, cloud service provider) instead of by the IoT product. If an organization is planning to acquire a constrained IoT product (i.e., the device has limited internal memory, storage, and/or processing power), the organization may need to carefully consider those capabilities that can be provided by the IoT product and those capabilities that will need to be provided by other system elements. Organizations should also carefully consider the key cybersecurity requirements for an IoT product that *must* be present on the product for it to be integrated into the system.

3.3.2. Identifying Requirements using Other Resources

In addition to IoT product cybersecurity capabilities and non-technical supporting capabilities identified using the mapping described in Sec. 3.3.1, organizations may determine that additional capabilities are needed from IoT products and/or system elements in order to support security controls and reduce risk to acceptable levels. The NISTIR 8259 series of documents, CSF, RMF, and other activities and resources can help organizations identify additional needed capabilities.

Guidelines that identify applicable starting-points for IoT product cybersecurity requirements may help some organizations overcome challenges they may encounter when determining appropriate IoT product cybersecurity requirements. Organizations must hit a moving target in identifying IoT product cybersecurity requirements to support a set of controls that may change based on the IoT product selected and its use case. Further compounding this challenge is the need for thorough understanding and consideration of a number of areas (e.g., technical knowledge about cybersecurity, knowledge of the operational side of the system/device, insight into organizational security controls), which may be spread among multiple personnel within an organization or fall outside their cybersecurity work role and related expertise. Small organizations, those geographically further from headquarters, and those with significant proportions of personnel without technological or cybersecurity work roles, among other factors may find these challenges are amplified.

NISTIR 8259A [24] specifies the high-level device technical cybersecurity capabilities that generally achieve minimal securability for most customers. The IoT core baseline, as the IoT product cybersecurity capability core baseline from NISTIR 8259A is called, is meant to apply to all IoT use cases and customers, meaning it is phrased at a high level to meet many different needs. NISTIR 8259B [25] presents a set of non-technical supporting capabilities—the IoT non-technical supporting capability core baseline—generally needed from manufacturers or entities to support common security controls. Like 8259A, the non-technical capabilities in 8259B are phrased at a high level to be broadly applicable to various use cases and customers.

The IoT core baselines presented in NISTIR 8259A and 8259B can be profiled for a specific customer, sector, or use case. The process of profiling tailors and/or extends the IoT core baselines and can be performed at any level of specificity, even to an individual customer (e.g., organization within the federal government).

One such profile of the IoT core baselines that is guided by the needs and goals of organizations is called the federal profile, which is included as Appendix A to SP 800-213A [18]. The federal profile uses the SP 800-53 Rev. 5 controls catalog [7] as an input source of federal government security needs and goals to identify IoT product cybersecurity capabilities and non-technical supporting capabilities. Since the federal profile targets minimal securability for all federal government use cases, it focuses on IoT product cybersecurity requirements that support the low-impact baseline set of SP 800-53 Rev. 5 controls, which would be a sub-set of the IoT product cybersecurity requirements in Sections 2 and 3 of SP 800-213A. This focus for the federal profile is based on the assumption that the low-impact baseline set of controls will be used as the minimum set of controls for systems either directly or as a sub-set of the full set of controls used (e.g., if the organization uses the moderate or high impact baseline or employs additional tailoring beyond the baseline). The federal profile is therefore recommended as a starting point for organizations to use to identify IoT product cybersecurity requirements when incorporating an IoT product into a low-impact system.

The federal profile, and other similar lists of capabilities that may be more applicable to the specific use case or deployment, can be helpful for organizations to reduce the challenges they may face in determining IoT product cybersecurity requirements. However, the federal profile and other lists of IoT product cybersecurity requirements may not be a perfect fit for a specific IoT product, organization, and/or system. The list of IoT product cybersecurity capabilities and non-technical supporting capabilities in the federal profile may still need to be tailored as described in Sec. 3.3.1. In particular, the use of the low-impact baseline may not be appropriate for all organizations and use cases (e.g., if the IoT product is to be integrated into a moderate- or high-impact information system). Tailoring of IoT product cybersecurity requirements derived from profiles, including the federal profile, using any available information such as organization-specific considerations will help alleviate possibly costly issues when seeking approval for or integrating the IoT product (e.g., having to procure another IoT product when the IoT product purchased cannot be approved or connected to the system as intended). This underscores the importance of involving IT personnel to ensure an evaluation of features and functionality pertinent to being able to securely configure or integrate a product, prior to a purchase being made.

Using the guidelines described in Sec. 3.3, organizations shall identify all applicable IoT product cybersecurity requirements, including *key cybersecurity requirements*, ensuring that information system security controls are supported. If the IoT product and/or manufacturer do not provide all required IoT product cybersecurity capabilities and non-technical supporting capabilities, organizations should follow established risk management strategies to plan for the IoT product's incorporation into the system. Section 4 discusses these risk mitigation options.

4. Understanding Risk Management Options for IoT Products

When preparing to acquire an IoT product, an organization may find that available IoT products on the market do not provide some of the needed IoT product cybersecurity requirements. Sometimes, organizations may also find that an IoT product lacks needed IoT product cybersecurity requirements after purchasing the equipment. These situations, where the IoT product does not support all IoT product cybersecurity requirements, do not necessarily preclude an organization from using the IoT product, but rather, indicates additional considerations are necessary to ensure appropriate use. In the same way that IoT products and their characteristics may affect risks, they may also affect appropriate mitigations for risk. This section focuses on how organizations can understand, plan for, and document the ways in which IoT products may affect appropriate risk mitigations.

Another important point is that an IoT product might still be securely used by an organization even if it doesn't provide all identified IoT product cybersecurity requirements. In some use cases, the organization might determine that an identified IoT product cybersecurity requirement is unnecessary for support of a control (e.g., if the IoT product does not function in a way that needs the protection addressed in the security control). The security control may still be supported by most elements of the system, but this IoT product justifiably (i.e., without introducing unacceptable risk) lacks the capabilities to support that security control. In another instance, the IoT product may provide a capability that supports a security control, but not in the same way as an organization is accustomed to (e.g., the IoT product provides a unique identifier, but not in the format used by the organization) [24]. Options may also exist for organizations to gain the mission benefits of using an IoT product without introducing unacceptable risk due to gaps between identified IoT product cybersecurity requirements and the IoT product cybersecurity capabilities provided by IoT products on the market.

An organization may still determine that certain IoT product cybersecurity requirements cannot be missing from an IoT product (i.e., it is a key cybersecurity requirement). Such a determination could preclude use of an IoT product if no product is available that meets the requirements. Organizations can minimize this occurrence by considering all options at their disposal that may allow them to securely use an IoT product. Section 4.1 will describe the discrete ways an IoT product may present challenges related to meeting IoT product cybersecurity requirements. Section 4.2 follows on these challenges by discussing ways in which organizations, IoT products, and/or their manufacturers and supporting third-party entities may be able to manage those challenges.

4.1. Potential Challenges Meeting IoT Product Cybersecurity Requirements

Section 3 described how an organization can determine the necessary IoT product cybersecurity requirements for an IoT product. When an organization attempts to acquire an IoT product, the identified IoT product cybersecurity requirements can help guide the procurement process. Organizations can look for available IoT products (and manufacturers) on the market that provide as many IoT product cybersecurity requirements as possible within the target price point. Acquiring IoT products that provide more than just key cybersecurity requirements can help minimize challenges in supporting security controls later in the system's life, when support needed for security controls may change. In some circumstances, using an IoT product that goes beyond key cybersecurity requirements may not be an option because locating IoT products on the market that provide even those key requirements may be difficult. Many factors contribute to this, including, but not limited to:

- Heterogeneity in IoT use cases and solutions supported by IoT products. IoT products may be intended for vastly different environments or uses, which can create variability in existence and efficacy of IoT product cybersecurity requirements. In some cases, they may lack IoT product cybersecurity requirements because aspects of the use case interfere with the goal supported (e.g., for this product's intended use case, cybersecurity is outweighed by another concern like safety) or nature of the support provided (e.g., a certain requirement cannot be met due to technical or physical limitations).
- The intended customer base for an IoT product may be very broad, forcing a manufacturer to make choices about which capabilities to support in a product. The capabilities provided by the product may favor one customer's use case more than another customer's. This issue can be accentuated when an IoT product is being used by an *unintended* customer, who may find capabilities missing from the IoT product.
- The cost and complexity of providing capabilities in the IoT product may cause manufacturers to build fewer capabilities into products. These decisions may reduce expectations for capabilities provided by the IoT product and shift the cybersecurity responsibilities to other system elements, possibly utilizing alternative approaches and capabilities for achieving security needs and goals.
- Business and other non-security considerations (e.g., monetary cost) for the customer and manufacturer may affect the IoT product cybersecurity and non-technical supporting capabilities desired or delivered, which could sometimes be in conflict for a specific IoT product.

Details: NISTIR 8228 Identifies IoT Product Cybersecurity Challenges

Organizations can best assess and account for gaps in IoT product cybersecurity requirements in relation to a particular IoT product and use case, but having a general understanding of possible cybersecurity challenges that could be encountered by organizations when adopting an IoT product can help avoid common issues. Organizations can reference NISTIR 8228 [22] to learn about challenges they may face when integrating an IoT product and use this information to inform the product requirements identification process and the subsequent procurement and integration processes.

Gaps in support for IoT product cybersecurity requirements may manifest from technological, form, cost, and other factors of the product that do not easily support or allow such capabilities; gaps may exist even when there are not particular limitations on the product's capacity to achieve those requirements. For example, some IoT product manufacturers may simply not provide adequate documentation for a product and may be unresponsive to additional requests, or IoT products may be technically able to support a IoT product cybersecurity capability, but due to limited demand for such a capability, even from the federal government, the manufacturer may forgo or delay adding it. Available products may also have gaps in IoT product cybersecurity requirements that cannot be remedied through adding those capabilities for these reasons, but also for business reasons (e.g., original manufacturer is no longer operating or supporting the IoT product). For each IoT product cybersecurity capability or non-technical supporting capability desired in an IoT product, there are three possible scenarios:

1. The IoT product cybersecurity capability or non-technical supporting capability is present in the IoT product as the capability is stated.

2. The IoT product cybersecurity capability or non-technical supporting capability is not present as the capability is stated, but an alternative capability is provided that is intended to support the same goal (though not necessarily the same security control).

3. The IoT product cybersecurity capability or non-technical supporting capability is not present as the capability is stated, and no alternative capability to support the goal is provided.

These three scenarios do not account for why a capability is not present in an IoT product, nor do they determine whether a missing or alternative capability is acceptable. The organization must make that determination for each specific capability based on contextual information (e.g., organization’s risk appetite, IoT product options, available solutions). These three product capability support scenarios can be valuable for communicating with a product vendor about where there may be gaps between the organization’s desired IoT product cybersecurity requirements and the capabilities provided by the IoT product or other IoT product components. Other IoT ecosystem participants (e.g., vendors, manufacturers) may be aware of and support sets of IoT product cybersecurity requirements, but these sets may not entirely align with an organization’s expectations. For example, some IoT product manufacturers may use the Federal Profile of the IoT Device Cybersecurity Baselines to build towards in an attempt to meet as many federal customers’ IoT product cybersecurity requirements as they can at time of design and development. Other manufacturers may use open standards or standards-based conformity and/or labelling mechanisms to determine presence and suitability of IoT product cybersecurity requirements. This set of capabilities, like any, is based on some number of assumptions about an IoT product, customer, and system; these assumptions may not apply to the specific purchase. Clear understanding by an organization of which capabilities are present in and around the IoT product and how this compares to what is desired and expected will aid in overcoming challenges due to lack of support.

4.2. Managing Gaps in IoT Product Cybersecurity Requirements

There may be reasons why an IoT product does not provide all the capabilities desired by a customer. Some amount of specialization in the design of IoT products and their capabilities for organizations may be appropriate, but it is neither possible nor advisable for organizations to drive IoT product cybersecurity capabilities into all IoT products in all use cases. For example, organizations may require significantly more non-technical documentation than an average customer. Providing the additional documentation may be trivial or of acceptable cost for the manufacturer. In this situation, alteration of the non-technical supporting capability is acceptable. Under limited circumstances, some IoT product cybersecurity capabilities may likewise be easily modified for organizations, such as the inclusion of additional configuration capabilities. Other modifications desired by an organization to the IoT product's cybersecurity capabilities may not be possible to accommodate. Some IoT product cybersecurity capabilities may require a level of computing resources that is not supported by the IoT product. Changing such fundamental aspects of an IoT product (e.g., available computing resources) may not be physically or financially possible for the manufacturer.

Organizations should be strategic and deliberate in their planning for IoT product cybersecurity requirements, including how to mitigate gaps between desired cybersecurity requirements and the capabilities provided by the IoT product. As organizations examine IoT products available on the market, they shall determine which IoT product cybersecurity requirements are provided by the IoT product (or manufacturer/third party in the case of non-technical supporting capabilities). The organization can make the following determinations as to how any gaps in capability support impact the organization's use of the IoT product:

1. Determine that the capability's support for the security control is justifiably missing from the IoT product and document as such. Justifiable reasons include:

    a. The goal of the security control does not apply to the proposed use case,
    b. Another security control that does not require direct support from the IoT product/manufacturer may be selected, or
    c. The residual risk introduced by the lack of support for the security control is acceptable to the organization.

2. Determine that support for the security control provided by an alternative capability is acceptable and requires no change in security control.

3. Determine that support provided by an alternative capability is acceptable but requires a change in security control.

4. Determine that the IoT product's lack of support or alternative support for the security control is unacceptable.

As summarized in Figure 14, three of the four determinations mean an organization can likely integrate the product despite the gap in IoT product cybersecurity capability. There are nuances to each determination that must be considered by organizations in deciding whether a specific IoT product cybersecurity requirement gap means they can or cannot integrate the IoT product.

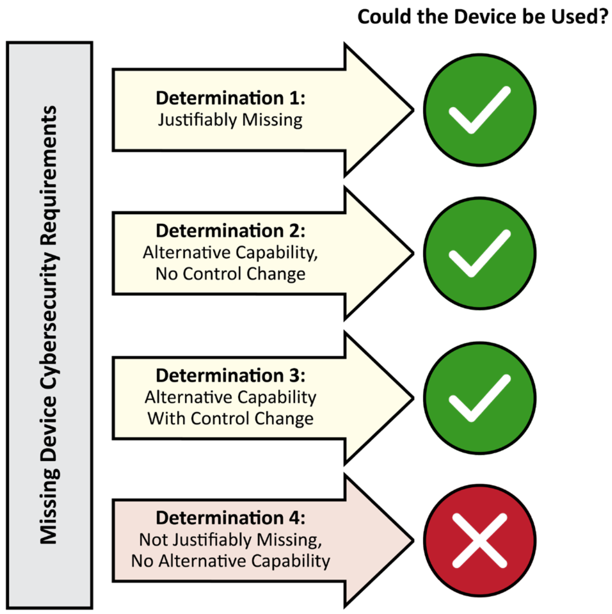

Figure 14: Likely Outcomes for Organizations based on the Four Determinations Discussed

For the first determination, an organization acknowledges the lack of an IoT product cybersecurity requirement but accepts the deficiency. In some instances, the goal of the security control and the security control itself may still apply to the system, but the IoT product will not directly support the security control as will other elements of the system. Alternatively, the organization may acknowledge that risk is introduced by the IoT product's lack of a capability to support the security control but that the risk is minimal and acceptable. These decisions of acceptable deviation from anticipated support for system security controls from the IoT product should be documented by organizations.

The second and third determinations involve the use of an alternative capability and/or security control than originally intended by the organization. The second determination is the simpler of the two since it does not require a change in security control but rather a different capability to support the security control. For example, the IoT product may use an authentication mechanism to verify a person's identity that is of a different, but acceptable, modality than the mechanism the organization typically uses (e.g., the IoT product uses derived PIV credentials rather than PIV cards to authenticate a person's identity). The organization may determine that the IoT product's alternate modality will satisfy the security control even though it initially appeared as a gap in requirements.

The third determination involves the organization selecting a compensating security control for the information system. This compensating security control better matches the capability(ies) provided by the IoT product while still addressing the same security goal to manage risk. However, selecting a compensating security control may not be possible for a variety of reasons. The compensating security control may be too costly to implement in the system or may not reduce risk to acceptable levels to justify the cost. Beyond financial considerations, some organizations may not be able to implement alternate security controls due to logistical, business, statutory, or other reasons. If the control or compensating control cannot be implemented for the system or IoT product, the product could only be used if the organization (i.e., authorizing official) accepts the residual risk. Ideally, the organization will be able to implement the security control, allowing use of the IoT product.

For the fourth determination, the IoT product cannot be used by the organization *as intended* because of the lack of the capability. This would be the determination if an IoT product lacks a key cybersecurity requirement, where the organization has identified those IoT product cybersecurity requirements that must be met (i.e., not omitted or replaced with an alternative) by an IoT product and its manufacturer and supporting entities to be considered "securable" by the organization. The organization should consider other ways the IoT product could be used in their operations. For example, an organization may intend to deploy the IoT product directly to the system as a peer with other elements. If the IoT product does not provide adequate support for allocated security controls via IoT product cybersecurity capabilities, the IoT product may not be securable by the organization in that intended use case. Rather than forgoing the IoT product entirely (i.e., Determination 4), the organization may consider the use of techniques such as network segmentation to logically separate the IoT product from the rest of the system (i.e., Determination 2 or 3). This separation may allow the organization to still realize the benefits of the IoT product while reducing both the risk introduced by the IoT product and the IoT product cybersecurity capabilities needed from the IoT product. It is recommended that organizations carefully consider strategies for how risk introduced by the IoT product can be reduced and how the IoT product can be securely introduced to the information system.

References

[1] Liu F, Tong J, Mao J, Bohn RB, Messina JV, Badger ML, Leaf DM (2011) NIST Cloud Computing Reference Architecture. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 500-292. https://doi.org/10.6028/NIST.SP.500-292

[2] Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18, Rev. 1. https://doi.org/10.6028/NIST.SP.800-18r1

[3] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[4] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[5] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[6] Souppaya MP, Scarfone KA (2022) Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 4. https://doi.org/10.6028/NIST.SP.800-40r4

[7] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[8] Joint Task Force (2020) Control Baselines for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53B, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53B

[9] Barker EB, Chen L, Roginsky AL, Vassilev A, Davis R (2018) Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56A, Rev. 3. https://doi.org/10.6028/NIST.SP.800-56Ar3

[10] Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v1r1

[11] Stouffer KA, Pease M, Tang CY, Zimmerman T, Pillitteri VY, Lightman S, Hahn A, Saravia S, Sherule A, Thompson M (2023) Guide to Operational Technology (OT) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-82r3. https://doi.org/10.6028/NIST.SP.800-82r3

[12] Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128, Includes updates as of October 10, 2019. https://doi.org/10.6028/NIST.SP.800-128

[13] Jansen W, Grance T (2011) Guidelines on Security and Privacy in Public Cloud Computing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-144. https://doi.org/10.6028/NIST.SP.800-144

[14] Mell PM, Grance T (2011) The NIST Definition of Cloud Computing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-145. https://doi.org/10.6028/NIST.SP.800-145

[15] Ross RS, McEvilley M, Winstead M (2022) Engineering Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-160v1r1. https://doi.org/10.6028/NIST.SP.800-160v1r1

[16] Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R (2021) Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-160v2r1

[17] Boyens JM, Smith AM, Bartol N, Winkler K, Holbrook A, Fallon M (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-161r1-upd1, Includes updates as of November 01, 2024. https://doi.org/10.6028/NIST.SP.800-161r1-upd1

[18] Fagan MJ, Megas KN, Marron JA, Brady KG, Jr., Cuthill BB, Herold R, Lemire D, Hoehn B (2021) IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-213A. https://doi.org/10.6028/NIST.SP.800-213A

[19] Committee on National Security Systems (2015) Committee on National Security Systems (CNSS) Glossary. (National Security Agency, Ft. Meade, MD), CNSS Instruction (CNSSI) No. 4009. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[20] National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

[21] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) NIST FIPS 200. https://doi.org/10.6028/NIST.FIPS.200

[22] Boeckl KR, Fagan MJ, Fisher WM, Lefkovitz NB, Megas KN, Nadeau EM, Piccarreta BM, Gabel O'Rourke D, Scarfone KA (2019) Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8228. https://doi.org/10.6028/NIST.IR.8228

[23] Fagan MJ, Megas KN, Cuthill BB, Marron J, Hoehn B (2026) Foundational Cybersecurity Activities for IoT Product Manufacturers. (National Institute of Standards and Technology,

Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8259r1. https://doi.org/10.6028/NIST.IR.8259r1

[24] Fagan MJ, Megas KN, Scarfone KA, Smith M (2020) IoT Device Cybersecurity Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259A. https://doi.org/10.6028/NIST.IR.8259A

[25] Fagan MJ, Marron JA, Brady KG, Jr., Cuthill BB, Megas K, Herold R (2021) IoT Non-Technical Supporting Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259B. https://doi.org/10.6028/NIST.IR.8259B

[26] Quinn SD, Chua J, Ivy N, Gardner RK, Kent KA, Smith MC, Witte GA (2025) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8286r1. https://doi.org/10.6028/NIST.IR.8286r1

[27] International Organization for Standardization (2015) *ISO 9000:2015 – Quality management systems — Fundamentals and vocabulary* (ISO, Geneva, Switzerland). Available at https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v1:en

[28] International Organization for Standardization/International Electrotechnical Commission (2023) *ISO/IEC 15288:2023 – Systems and software engineering – System life cycle processes* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/81702.html

[29] Petersen R, Santos D, Wetzel KA, Smith MC, Witte GA (2020) Workforce Framework for Cybersecurity (NICE Framework). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1. https://doi.org/10.6028/NIST.SP.800-181r1

[30] Souppaya MP, Scarfone KA, Dodson DF (2022) Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-218. https://doi.org/10.6028/NIST.SP.800-218

[31] Badger ML, Grance T, Patt-Corner R, Voas JM (2012) Cloud Computing Synopsis and Recommendations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-146. https://doi.org/10.6028/NIST.SP.800-146

[32] Rose SW, Borchert O, Mitchell S, Connelly S (2020) Zero Trust Architecture. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-207. https://doi.org/10.6028/NIST.SP.800-207

[33] Voas JM (2016) Networks of 'Things'. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-183. https://doi.org/10.6028/NIST.SP.800-183

[34] Simmon E (2020) Internet of Things (IoT) Component Capability Model for Research Testbed. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8316. https://doi.org/10.6028/NIST.IR.8316

Appendix A. List of Abbreviations, and Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

CSF
Cybersecurity Framework

DDoS
Distributed Denial of Service

EO
Executive Order

FIPS
Federal Information Processing Standards

FISMA
Federal Information Security Modernization Act

IoT
Internet of Things

IT
Information Technology

ITL
Information Technology Laboratory

NICE
National Initiative for Cybersecurity Education

NIST
National Institute of Standards and Technology

OMB
Office of Management and Budget

OT
Operational Technology

PIV
Personal Identity Verification

RMF
Risk Management Framework

SP
Special Publication

SSDF
Secure Software Development Framework

Appendix B. Glossary

Capabilities Catalog
Comprehensive list of IoT product cybersecurity capabilities derived from analysis of comprehensive list of source documents for the application or sector.

> *Note 1: For the federal sector, NIST SP 800-53 Rev. 5 [7] provided the definition of controls used to create the NIST-generated capabilities catalog used for the Federal profile.*

Configuration
The possible conditions, parameters, and specifications with which an information system or system component can be described or arranged. The Device Configuration capability does not define which configuration settings should exist, simply that a mechanism to manage configuration settings exists.[[12], Adapted]

Core Baseline
A set of technical capabilities needed to support common cybersecurity controls that protect the customer's devices and device data, systems, and ecosystems.

Customer
The organization or person that receives a product or service. [26]

IoT Product Cybersecurity Capability
Cybersecurity features or functions that IoT computing products provide through their own technical means (i.e., product hardware and software).

Device Cybersecurity Capability Core Baseline
See *core baseline*.

Device Identifier
A context-unique value—a value unique within a specific context—that is associated with a device (for example, a string consisting of a network address). [[9], adapted]

Entity
A person, device, service, network, domain, manufacturer, or other party who might interact with an IoT product.

Federal Profile
Profile of the IoT device cybersecurity capability core baseline [24] and non-technical supporting capability core baseline [25] to provide security guidelines for federal government organizations related to IoT products.

Interface
A boundary between the IoT product components and entities where interactions take place. There are two types of interfaces: network and local. [CNSSI, Adapted]

Local Interface
An interface that can only be accessed physically, such as a port (e.g., USB, audio, video/display, serial, parallel, Thunderbolt) or a removable media drive (e.g., CD/DVD drive, memory card slot).

Key Cybersecurity Requirement
An IoT product cybersecurity requirement that if lacking from an IoT product (in the case of a IoT product cybersecurity capability) or manufacturer or supporting entity (in the case of a non-technical supporting capability) will result in unacceptable risk to the organization.

Network Interface
An interface that connects the IoT device to a network.

Non-Technical Supporting Capability
Non-technical supporting capabilities are actions an organization performs in support of the cybersecurity of an IoT device.

Non-Technical Supporting Capability Core Baseline
The non-technical supporting capability core baseline is a set of non-technical supporting capabilities generally needed from manufacturers or other third parties to support common cybersecurity controls that protect an organization's devices as well as device data, systems, and ecosystems.

Profile
A profile is a baseline set of minimal cybersecurity requirements for mitigating described threats and vulnerabilities, as well as supporting compliance requirements for a defined scope and type of a particular use case (e.g., industry, information system(s)), using a combination of existing cybersecurity guidance, standards and/or specifications baseline documents or catalogs. A profile organizes selected guidance, standard(s) and/or specification(s) and may narrow, expand and/or otherwise tailor items from the starting material to address the requirements of the profile's target application.

Software
Computer programs and associated data that may be dynamically written or modified during the device's execution (e.g., application code, libraries). [[7], Adapted]

Update
A patch, upgrade, or other modification to code that corrects security and/or functionality problems in software. [[6], adapted]

Appendix C. Change Log

This draft has been updated from the original publication of SP 800-213 based on developments over the years since that document's final publication. In this revision, the focus shifts from IoT devices to IoT products, which prompted several changes:

- Language is updated throughout the document to be product-focused.
- IoT products are described, and their potential components are discussed in Section 2.
- Additional background and perspectives (including new graphics) for system-product interactions are added to Section 2.

NIST also heard feedback that additional connections to NIST guidelines and external publications would be beneficial to readers, and so some were added, including extended discussion in Section 2 of two NIST guidelines that can help inform readers. On this point, NIST heard additional feedback that SP 800-213 should be helpful for the variety of ways an organization may be deploying IoT products and thus are working to identify cybersecurity requirements. The additional discussion of NIST guidelines are intended to help inform readers who may be essentially creating an "IoT product" from off-the-shelf components to meet a very specific or otherwise niche use case or who may be deploying a large number of IoT products into a coordinated system.

Beyond content, the template has been updated to the most current, and call-out boxes have been organized into two types to help identify whether the content contains considerations for readers or provides additional detail.