NIST Special Publication 800-213

IoT Device Cybersecurity Guidance for the Federal Government:

Establishing IoT Device Cybersecurity Requirements

Michael Fagan
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
Katerina N. Megas
Rebecca Herold
David Lemire
Brad Hoehn

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

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

NIST Special Publication 800-213

IoT Device Cybersecurity Guidance for the Federal Government:

Establishing IoT Device Cybersecurity Requirements

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

Rebecca Herold
The Privacy Professor
Des Moines, IA

David Lemire
Brad Hoehn
Huntington Ingalls Industries
Annapolis Junction, MD

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

November 2021

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-213
Natl. Inst. Stand. Technol. Spec. Publ. 800-213, 47 pages (November 2021)
CODEN: NSPUE2

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

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Comments on this publication can be submitted to:

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

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

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.

Abstract

Organizations will increasingly use Internet of Things (IoT) devices for the mission benefits they can offer, but care must be taken in the acquisition and implementation of IoT devices. This publication contains background and recommendations to help organizations consider how an IoT device they plan to acquire can integrate into a system. IoT devices and their support for security controls are presented in the context of organizational and system risk management. This publication provides guidance on considering system security from the device perspective. This allows for the identification of device cybersecurity requirements—the abilities and actions an organization will expect from an IoT device and its manufacturer and/or third parties, respectively.

Keywords

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

Supplemental Content

The NIST Cybersecurity for IoT Team has undertaken an effort that aims to help manufacturers and federal government organizations better understand the device cybersecurity capabilities and supporting non-technical capabilities that may be needed from or around IoT devices used by federal government organizations. To that end, NIST has developed a catalog of IoT device cybersecurity capabilities and supporting non-technical capabilities for manufacturers and IoT device customers. The catalog identifies technical and non-technical capabilities that may be necessary for supporting NIST SP 800-53 Rev. 5 [800-53] 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 device. Ultimately, the goal is to enable organizations to securely incorporate IoT devices into their systems and meet their security requirements. The catalog can be found in SP 800-213A, *IoT Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog* [800-213A].

Acknowledgments

The authors wish to thank all contributors to this publication, including the participants in workshops and other interactive sessions; the individuals and organizations from the public and private sectors, including manufacturers from various sectors as well as several manufacturer trade organizations, who provided feedback on the preliminary public content; and colleagues at NIST who offered invaluable inputs and feedback. Special thanks to the NIST Risk Management Framework team for their extensive feedback.

Audience

The target audience of this publication is information security professionals, system administrators, and others in organizations tasked with assessing, applying, and maintaining security on a system.

Patent Disclosure Notice

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents, and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Table of Contents

List of Appendices

List of Figures

1 Introduction

As Internet of Things (IoT) technology evolves, it is inevitable that most organizations[1] will integrate this equipment into systems[2]. IoT[3] technology creates many opportunities for organizations in support of mission objectives. IoT technology may also present security challenges throughout the lifecycle if proper considerations are not made during the acquisition and integration of an IoT device.

Existing NIST risk management guidance helps organizations identify, communicate, and satisfy the security requirements[4] to support mission and business functions and manage risk across the organization from the system level to the organizational level. 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[5]. IoT devices used by organizations will frequently be integrated as system elements, and this integration will often happen well after the information system has been initially deployed. It is important that organizations identify support for system and organizational security capabilities needed from individual system elements (e.g., IoT devices) to help manage risk to the system to which they connect. As an example, an organization may purchase voice-activated printers and integrate them into the existing enterprise network. Organizations must also grapple with the challenge that many IoT devices lack features and functions that are common in conventional information

[1] Like other NIST guidance, *organization* is meant to describe entities of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).

[2] 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 guidance [800-18, 800-30, 800-37, 800-39, 800-60] and FIPS 200 [FIPS-200], 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; …” [800-37] 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 devices naturally bring many connections to a system through their actuation and networking capabilities. Any *system* that includes an IoT device as a system element will find value in this publication. Systems that do not incorporate IoT devices may find value in the guidance within this publication, but some concepts and discussion may not be applicable to or align with the system of interest.

[3] Definitions of IoT vary, but generally agree that IoT technology bridges operational technology such as sensors and actuators with information technology such as data processing and networking. This document uses the same definition/scope for an IoT device that appears in prior Cybersecurity for IoT work such as NISTIR 8228 [IR8228] and NISTIR 8259 [IR8259]. NISTIR 8228 Section 2 provides additional detail on how device capabilities are understood relative to IoT devices.

[4] 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.” [800-53]

[5] 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.

technology (IT) equipment. This lack of functionality in IoT devices can cause security concerns; for example, an IoT device may lack the capability to update software.

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

1.1 Purpose and Applicability

This publication is intended to help organizations incorporate IoT devices into an existing information system as system elements. 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. The IoT devices in-scope for this publication can function on their own, although they may be dependent on other specific devices (e.g., an IoT hub) or systems (e.g., a cloud) for some functionality[6]. 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 guidance,[7] address those situations more directly.

1.2 Target Audience

The target audience of this publication is information security professionals, system administrators, and others in organizations tasked with assessing, applying, and maintaining security on a system. Personnel within the following Workforce Categories and Specialty Areas from the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity [NICE] 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

[6] This scope for IoT devices is taken from NISTIR 8259 [IR8259] and is a definition of IoT devices that has been well vetted and received by both the public and private sectors.

[7] See https://nist.gov/RMF for an overview of the NIST RMF and suite of supporting guidelines.

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 [800-18], 800-30 Rev. 1 [800-30], 800-37 Rev. 2 [800-37], 800-39 [800-39], 800-53 Rev. 5 [800-53], 800-60 Vol. 1 Rev. 1 [800-60], and 800-160 Vol. 1 [800-160v1] and Vol. 2 [800-160v2], as well as SP 800-82 Rev. 2 [800-82] and the NIST Cybersecurity Framework [CSF]. It also follows from the foundational cybersecurity for IoT work from NIST documented in NISTIR 8228 [IR8228] and the NISTIR 8259 series [IR8259, IR8259A, IR8259B]. Details on the relationship to these other publications is in Section 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, but 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 guidance that should be understood:

> This document contains guidance for federal organizations when acquiring and/or integrating an IoT device into an existing system.
>
> a. Where the term "shall" is used, the statement is to be interpreted as a *requirement*.
> b. 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 devices 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 device cybersecurity requirements.
- Section 4 describes how an organization can navigate security challenges that arise when IoT devices do not meet device cybersecurity requirements as anticipated.

2 Background Considerations

This section presents background information about IoT devices that organizations should consider in their device acquisition processes. This publication draws from other NIST guidance, namely the Risk Management Framework (RMF) [800-37], the Cybersecurity Framework (CSF) [CSF], and NIST SP 800-161, *Cyber Supply Chain Risk Management Practices for Systems and Organizations* [800-161]. Organizations familiar with this guidance and the context of IoT devices within a system could skip this section. It is expected that organizations will follow the RMF steps to manage risk to the system and organization throughout the system development life cycle. As IoT devices are introduced to the system, often after it is in operation, it is critical to consider the security impact of such changes. Since IoT devices will often be integrated into existing systems, this publication will provide guidance for organizations in the context of the RMF.

2.1 Systems and Elements

As discussed in Section 1, federal cybersecurity risk management processes generally consider the security of organizations and systems, and highlight that systems are made up of elements. Increasingly, IoT devices 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* [800-37]. Some of the key concepts, particularly those covered in section 2.4 of SP 800-37 Rev. 2, will be highlighted here. Figure 1 shows these concepts visually, adapted from a figure in SP 800-37 Rev. 2, Revision 2.

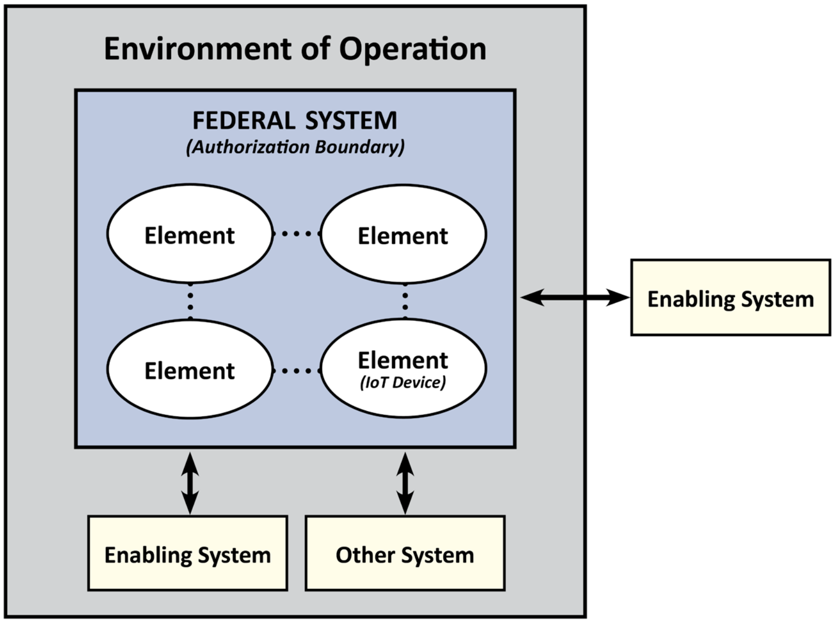


Figure 1: Visualization of the System and Environment

An information system "is a set of interacting elements that are organized to achieve one or more stated purposes." [ISO15288] Information systems are defined by the authorization boundary[8], 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.

As explained in SP 800-37 Rev. 2, organizations define and determine the parts of the environment of operation that are within the authorization boundary of each federal system. Figure 1 shows how the environment of operation can contain multiple authorization boundaries, including other systems and enabling systems. Elements, including IoT devices, may interact and communicate across multiple systems/authorization boundaries. However, for accountability and risk management purposes, each IoT device is only included within one authorization boundary.[9] Additional enabling systems will fall outside of the environment of operation (e.g., a system hosted by another organization or service provider). This concept of systems and elements can help clarify the ways IoT devices might be used by organizations and the subsequent identification of device cybersecurity requirements.

Some IoT devices should be characterized as an enabling or other system if the device is managed in a different authorization boundary than the organization's system.[10] 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.

[8] See SP 800-37, Section 2.5 and Appendix G for additional guidance on authorization boundaries for federal systems.

[9] 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 have to implement controls around their use of the sensor system's data to meet government-wide requirements.

[10] As discussed in SP 800-37 Rev. 2, 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 Rev. 2 goes further to note that the risk management of these kinds of systems would be "addressed within their respective authorization boundaries."

Cybersecurity Responsibility Related to Enabling and Other Systems

Considering an IoT device as an enabling or other system does not alleviate *all* cybersecurity considerations on the part of an organization. The IoT device 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 manufacturer of the device, third-party service provider). That organization (i.e., that manages the IoT device 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 SP 800-161 Revision 1, *Cyber Supply Chain Risk Management Practices for Systems and Organizations* [800-161] to understand these responsibilities and supporting practices.

Other IoT devices acquired by organizations will be best characterized as system elements that fall within the authorization boundary of an existing federal system. This is depicted in Figure 1 by the element in the bottom right corner of the authorization boundary. Since the device will be integrated as a system element, organizations may have significantly more expectations about how this IoT device must support the security controls of the information system and/or organization. Technical capabilities[11] may be expected from system elements (e.g., IoT devices) to support information system controls; similarly, organizations may depend on non-technical capabilities provided by manufacturers and/or third parties to support information system controls.

If the IoT device lacks technical and/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 and/or non-technical capabilities lacking in the IoT device might be provided by other 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 device limitations). If risk(s) introduced by the IoT device cannot be mitigated within the organization's risk tolerance level, the organization could accept these new risks or decide to not incorporate the IoT device into the information system.

This publication can apply to IoT devices in both scenarios (i.e., as an enabling/other system, or as an element of an existing system) but is primarily aimed at IoT devices as system elements since the organization typically has greater responsibility and control over these IoT devices. Understanding the IoT device's relationship to the system is important to properly define the device cybersecurity requirements needed to support organizational and system security requirements.

[11] Both technical capabilities and non-technical capabilities are discussed in Section 2.2.

2.2 How IoT Devices Support Security

The relationship of an IoT device to an information system provides the context to understand how an IoT device supports both system and organizational objectives. NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* [800-39], 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 SP 800-39, highlighting the connection between systems and elements as discussed in SP 800-37 Rev. 2 and Section 2.1 above. Figure 2 shows the connection between the concepts discussed in SP 800-39 and system elements.

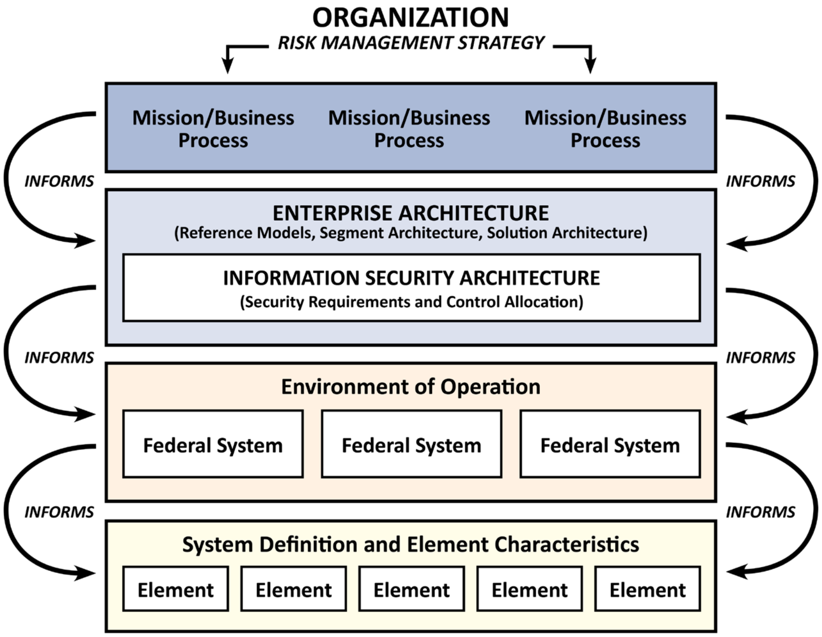


Figure 2: Information Security Requirements Integration to the Element Level

SP 800-39 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. The information security architecture informs the federal systems within the environments of operation, particularly through the application of security controls. This publication focuses on IoT devices as system elements that must both support and be informed by the system and its security controls.

The primary way that IoT devices support security controls is via technical means, which are called *device cybersecurity capabilities*[12]. *Non-technical supporting capabilities*, actions that manufacturers or third parties take in support of the initial and on-going security of IoT devices,

[12] Device cybersecurity capabilities, in the context of this document, are those technical capabilities that reside on the IoT device itself. Device cybersecurity capabilities are a subset of the technical capabilities needed to support system security controls. Technical capabilities may reside on other system elements or be provided by other or enabling systems.

are also critical for supporting security controls. The NISTIR 8259 series discusses the concept of device cybersecurity capabilities 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.

Example Device Cybersecurity and Non-Technical Supporting Capabilities

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

NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers* [IR8259], while focused on manufacturers, can help organizations consider their needs and goals related to IoT devices. In particular, NISTIR 8259 highlights how IoT devices 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 helping customers meet their cybersecurity needs and goals. In light of this, NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline* [IR8259A] provides a starting point of device 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* [IR8259B] 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.

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 NIST SP 800-53B, *Control Baselines for Information Systems and Organizations* [800-53B]. The IoT core baselines are distinct from the SP 800-53B security control baselines. The IoT core baselines define high-level device 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 device 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.

Both device 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 3 illustrates how device cybersecurity capabilities and non-technical supporting capabilities (grouped together as 'Device Cybersecurity Requirements') support system/organizational security capabilities, which in turn satisfy organizational security requirements.

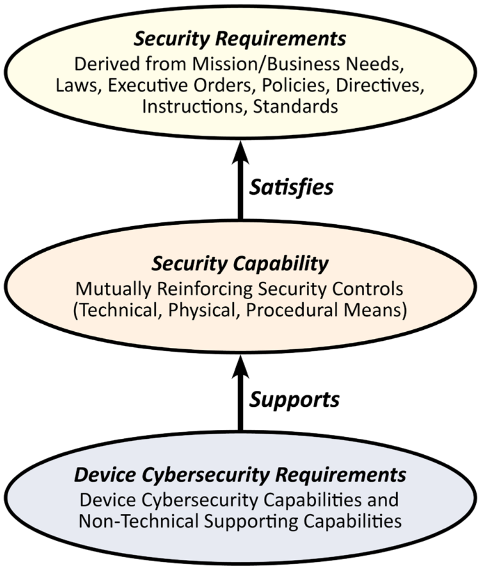

Security Requirements
Derived from Mission/Business Needs, Laws, Executive Orders, Policies, Directives, Instructions, Standards
Satisfies
Security Capability
Mutually Reinforcing Security Controls (Technical, Physical, Procedural Means)
Supports
Device Cybersecurity Requirements
Device Cybersecurity Capabilities and Non-Technical Supporting Capabilities

Figure 3: Role of Device 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[13]. Controls used by federal agencies are selected from NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* [800-53]. These controls are technology agnostic and can apply to IoT devices incorporated into systems as system elements.

[13] See SP 800-37 for more information and detailed task descriptions of the Select and Implement Steps.

IoT Devices in the Context of the Risk Management Framework

Understanding that an IoT device is a system element facilitates an understanding of how the IoT device must be considered in the risk management process. The acquisition and integration of an IoT device into an information system may alter the system's risk assessment based on new risks introduced by the device. An updated risk assessment may require additional or new controls to be selected and implemented in the system.

The guidance in this publication focuses on establishing device cybersecurity requirements to support security controls. This publication provides general considerations of how IoT devices may impact an information system's risk assessment and subsequent allocation of controls that may be necessary. Readers are encouraged to reference SP 800-30, Revision 1, *Guide for Conducting Risk Assessments* [800-30] and other publications in the RMF suite of publications for guidance on assessing risk due to the inclusion of an IoT device into an information system.

2.3 How IoT Devices May Create Security Challenges

Integrating an IoT device into a system can present a number of challenges for organizations. Organizations should strive to understand these challenges before an IoT device is acquired and integrated into a system. For example, due to a number of market and technological factors, IoT devices often lack cybersecurity functionality commonly present in conventional IT equipment (e.g., laptops). Sometimes, a lack of cybersecurity functionality in an IoT device or support from the manufacturer or supporting entities could introduce unacceptable levels of risk to the system, such as when an IoT device lacks a *key device cybersecurity requirement*. Key device cybersecurity requirements are those the organization has determined the IoT device must possess and/or manufacturers and supporting entities must provide in order for the device to be integrated in the system. Key device cybersecurity requirements are important to consider because without them, an IoT device cannot be considered "securable" by the organizations and will not be able to be used as intended or possibly at all. Other device cybersecurity requirements (i.e., those not considered key), if lacking from the IoT device or manufacturers and supporting entities, could possibly be compensated for with other device cybersecurity and/or non-technical supporting capabilities or other security controls entirely, giving organizations options when encountering challenges integrating and using IoT devices. Thus, organizations should consider all device 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 device or by the manufacturer and/or supporting entities.

NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* [IR8228] 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, the challenges faced could diverge from those explored in NISTIR 8228. Organizations are encouraged to apply the concepts in NISTIR 8228 to identify challenges applicable to their use cases.

Overview of NISTIR 8228 Concepts

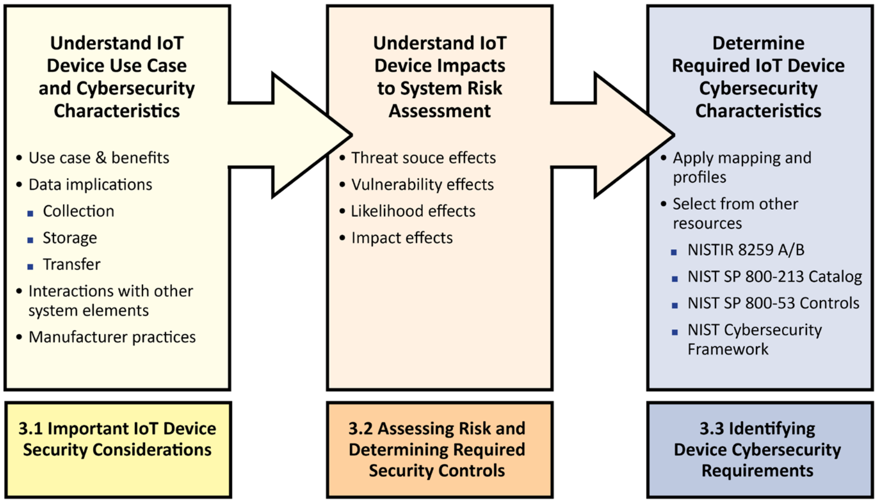
NISTIR 8228 explores a number of challenges, grouped around conventional risk mitigation areas such as asset management, data protection, incident detection, and vulnerability management. The publication further groups these areas into goals of protecting device security, data security, and/or individual 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 device into an information system. NIST SP 800-160, Volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* [800-160v1] 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, among others 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 IoT devices are added as system elements, organizations should consider how the integration of the IoT device could impact system and organizational security requirements. However, integrating an IoT device into an information system can also be aided by taking a device-centric perspective. Through a device-centric perspective, an organization can identify and articulate the device cybersecurity requirements (i.e., the set of device cybersecurity capabilities and non-technical supporting capabilities) required from IoT devices and manufacturers/third parties to support security capabilities and satisfy security requirements. Organizations should be aware that even if the articulated device 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 Device Cybersecurity Requirements for IoT Devices

This section provides guidance to organizations in determining the applicable device cybersecurity requirements (i.e., the set of device cybersecurity capabilities and non-technical supporting capabilities) for an IoT device.


Understand IoT Device Use Case and Cybersecurity Characteristics
• Use case & benefits
• Data implications
▪ Collection
▪ Storage
▪ Transfer
• Interactions with other system elements
• Manufacturer practices
Understand IoT Device Impacts to System Risk Assessment
• Threat souce effects
• Vulnerability effects
• Likelihood effects
• Impact effects
Determine Required IoT Device Cybersecurity Characteristics
• Apply mapping and profiles
• Select from other resources
▪ NISTIR 8259 A/B
▪ NIST SP 800-213 Catalog
▪ NIST SP 800-53 Controls
▪ NIST Cybersecurity Framework
3.1 Important IoT Device Security Considerations
3.2 Assessing Risk and Determining Required Security Controls
3.3 Identifying Device Cybersecurity Requirements

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

Each organization should develop a process for identifying and articulating IoT device cybersecurity requirements that aligns with their existing policies and procedures (e.g., acquisitions, security, system administration). The guidance presented in this publication provides a starting point for organizations—as well as additional resources organizations can use—in identifying IoT device cybersecurity requirements. The steps described in this section happen before an IoT device is purchased and/or integrated. At this stage, the IoT device 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 device and support limitations should be identified through further engagement with the available producers and vendors.

3.1 IoT Device Cybersecurity Considerations

The decision to integrate an IoT device into a system may occur for a variety of reasons (e.g., to achieve business objectives, further technical advancements, provide administrative support). The reason the IoT device is being acquired will influence 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 device 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 IoT devices, but this list is not exhaustive. The answers to these and other questions can ultimately help organizations assess risk and identify IoT device cybersecurity requirements for their use case(s). Accurately and completely answering these questions for many IoT devices will require consultation with IT personnel within the organization.

1. **What is the benefit of the IoT device and how will it be utilized?** Organizations can help ensure that device cybersecurity requirements receive proper consideration by establishing an explicit benefit for integrating the IoT device and understanding how the IoT device will be used. For example, if the IoT device 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.

2. **What data is collected?** IoT devices 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 IoT devices should be understood, but three main types of data may be of concern:

    a. *Personal data:* Many IoT devices can sense or collect data of, from, or about people, which can constitute personal data and represent privacy sensitive data.

    b. *Confidential organizational/Federal government data:* The IoT device may collect restricted or confidential data, which could influence its risk level. For example, IoT devices 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 devices 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.

3. **In what technologies will the data be stored and how will it be transmitted?** Many IoT devices maintain connections to cloud services and mobile/web applications that are central to the device's functionality. IoT devices can also connect to additional external services, which may be provided and hosted by a number of third parties. Organizations

should consider where the IoT device might store data —in the device, the manufacturer's network, a manufacturer-contracted entity's network (e.g., cloud service provider[14]), etc. In addition, organizations should consider how the data will be secured in transit as connections to external services and third parties are made and used.

4. **In what geographic areas will the data be shared and/or stored?** The architecture that supports IoT devices is increasingly global. Organizations should consider where data from prospective IoT devices will be transmitted and stored to ensure applicable security requirements are met. An IoT device 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.

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

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

1. **Might the device interfere with other aspects of operations or system functionality?** Unlike conventional IT equipment, IoT devices are more likely to interact with the physical world through sensing and/or actuating. This interaction increases the possibility that an IoT device could affect 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 device introduce privacy or safety risks for people?* IoT devices could collect and share sensitive data about people, including, but not limited to, audio and video data. An IoT device 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 device may introduce privacy or safety risks is critical to planning for risk mitigation.

    b. *Could the IoT device interfere with system reliability or resiliency?* The diversity of IoT device use cases also creates the possibility that the IoT device's expected operational environment may vary from where it is actually deployed. In such an instance, the IoT device might negatively interact with other system elements or

[14] As a reminder to organizations, 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* [800-144] for additional guidance on cloud security considerations, as well as SPs 800-145, *The NIST Definition of Cloud Computing* [800-145] and 800-146, *Cloud Computing Synopsis and Recommendations* [800-146] for additional guidance on cloud computing and storage technologies. Finally, NIST SP 500-292, *NIST Cloud Computing Reference Architecture* [500-292] may be a useful additional resource for organizations.

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 devices may not be as digitally and physically resilient as their IT or OT counterparts since IoT devices 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 device.

2. **Would the IoT device introduce unacceptable risks to the organization or result in non-compliance with cybersecurity requirements?** Some IoT devices 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 device use case and whether the risk introduced is acceptable. In some use cases, the IoT device 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 device have known security and/or privacy vulnerabilities?** Like all connected products, IoT devices attract attention from security professionals and researchers who identify security and/or privacy concerns. Manufacturers also commonly publish similar information concerning their devices. Understanding known vulnerabilities can inform an organization's acquisition, risk assessment, and possible integration of an IoT device. For example, if known vulnerabilities exist that the manufacturer cannot mitigate, organizations would have to identify and address risks introduced by the IoT device through other means.

As discussed extensively in NISTIR 8228, 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 device will create any security and privacy challenges for the information system and organization. One common way challenges arise is when an IoT device does not fully support *key device cybersecurity requirements*. Organizations may reduce these challenges by considering important aspects of how the IoT device should connect and function to ensure the device conforms with expectations, and, thus, may define, inform, or otherwise impact key device cybersecurity requirements. In particular, organizations should consider:

1. **What organization-specific information is important to defining key device cybersecurity requirements?** Organizations often invest in specific solutions or implementations that would be the preferred support for various security controls. Identifying this kind of organizational information can help guide a purchase and reduce conflicts in applying security controls if the IoT device is integrated into a system. Since IoT devices 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 information can

impact what is acceptable to an organization, which mitigations are practical and appropriate, and the determination of device cybersecurity requirements. Some examples of organization-specific information include, but are not limited to:

1. *Does the organization require Personal Identity Verification (PIV) card-based authentication or does it allow password-based 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 device 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)[15].

2. *Does the organization purchase products from particular manufacturers or 3rd parties?* Such situations may limit the IoT devices readily available to the organization. This may, in turn, limit availability of IoT devices 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 device 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 device lack key device cybersecurity requirements?** Key device cybersecurity requirements are those the organization has determined that the IoT device must possess in order for the device to be integrated in the system and make external connections to other systems or the Internet. Lack of key device cybersecurity requirements indicates that the IoT device cannot support existing information system controls, which subsequently introduces unacceptable levels of risk[16]. To support information system security controls, the organization may need to consider if other system elements (e.g., a gateway, hub, cloud service) can provide the capabilities missing from the IoT device but should keep in mind those *key* device cybersecurity requirements

[15] 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.

[16] Since key device 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 [IR8286]). A higher risk appetite when using the IoT device may lead to fewer key device 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 device cybersecurity requirements and thus not willing to omit the requirement if lacking from an IoT device. Proper understanding of risk appetite and other cybersecurity considerations will require input from IT security personnel.

that cannot be provided elsewhere, otherwise compensated for, or omitted without introducing unacceptable risk to the organization.

3. **Will the implementation or maturity of device cybersecurity capabilities and/or non-technical supporting capabilities fail to satisfy key device cybersecurity requirements?** Some IoT devices may completely lack key device cybersecurity requirements, potentially making the IoT device unusable by the organization. Other IoT devices may provide device 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 device's cybersecurity capabilities lack maturity, the task of securing the device 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 device and how do they relate to key device cybersecurity requirements?** An understanding of how the IoT device will interact with the digital and physical worlds is important to understanding whether the device 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 device must connect to can help an organization ensure all connections the device 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 device for maintenance or diagnostics may conflict with how some devices are deployed (e.g., if they must be placed in an inaccessible location making physical maintenance difficult or impossible).

In addition to the specifics of the device and how it works, organizations should also consider the practices of the manufacturer in the development and on-going support of the IoT device. 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[17] and supply chain practices[18] to support their operations?** The use of secure development and supply chain practices in the manufacture of IoT devices will not solve all cybersecurity issues but will help reduce

[17] Additional information and guidance on secure development as it relates to software can be found in NIST's *Secure Software Development Framework* (SSDF) [SSDF].

[18] More guidance 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 SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* [800-161].

cybersecurity issues with IoT devices and provide additional assurances to organizations of the cybersecurity posture of the manufacturer and IoT device.

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.

The questions in this section assist organizations in understanding key aspects of the use case of the proposed IoT device 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 device 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 devices that may help organizations determine the risk associated with an IoT device. Organizations assess risk to IoT devices using the organization-defined approach based on guidance in NIST SP 800-30 but supplement the risk model for IoT using the guidance in this section.

Figure 5 below illustrates how to update a risk model specifically for an IoT device, closely aligned and adapted from the risk model with key risk factors identified in SP 800-30 Rev. 1 [800-30]. This updated risk model would then be used with other information to assess risk to the system, including the IoT device as an element.

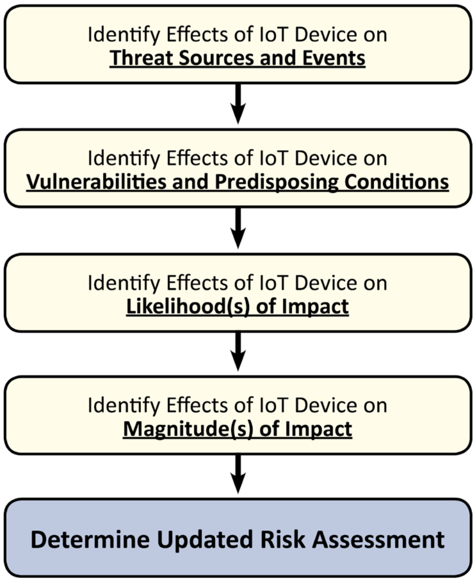

Identify Effects of IoT Device on Threat Sources and Events
Identify Effects of IoT Device on Vulnerabilities and Predisposing Conditions
Identify Effects of IoT Device on Likelihood(s) of Impact
Identify Effects of IoT Device on Magnitude(s) of Impact
Determine Updated Risk Assessment

Figure 5: Steps to Updating a Risk Model and Risk Assessment using New Information about an IoT Device.

Ideally the inclusion of an IoT device 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 device. The following discussion of threats, vulnerabilities, likelihood, and impact shall be considered by an organization as part of the risk model of an IoT device 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 device affect the threat sources and events that must be considered as part of a risk assessment? An IoT device 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 devices 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 devices may also not face the same threat sources and events that the rest of a system might. For example, IoT devices 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 devices will often have many of the same threat sources and events as the existing information system. There may be a set of unique IoT device threat sources and events as well as some information system threat sources and events that do not apply to the IoT device.

In this sense, there are two classes when comparing threat sources and events between the IoT device and information system: the threat sources and events can be the *same* or *different*. *Same* means the sets are identical such that the IoT device 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 device affect vulnerabilities and predisposing conditions considered as part of a risk assessment? As defined in CNSSI[19] 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." [CNSSI] 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 device. Alternatively, considering potential vulnerabilities in an IoT device (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 DDoS[20]-executing botnet may have existed before, but a proposed IoT device deployment within the system may introduce vulnerabilities (e.g., default credentials) and predisposing conditions for this threat to exploit. IoT devices may have many of the same vulnerabilities as the existing information system. There may be a set of unique IoT device vulnerabilities as well as some information system vulnerabilities that do not apply to the IoT device.

In this sense, there are two classes when comparing vulnerabilities and predisposing conditions between the IoT device and information system: they can be the *same* or *different*. *Same* means the sets are identical such that the IoT device 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:

[19] Committee on National Security Systems Instructions

[20] Distributed Denial of Service

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 device affect likelihood(s) of occurrence 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)." [CNSSI] 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 device 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 device on likelihood of occurrence can be expressed as being *greater*, *lower*, or *equal* to the likelihood of occurrence without the IoT device. For example, an IoT device 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 device can be said to have *greater* likelihood of occurrence compared to the system without the IoT device. Conversely, an IoT device 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 device*. In some instances of threats and vulnerabilities, the designation of a lower likelihood of occurrence may apply only to the IoT device, 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 device is lower[21].

[21] A risk assessment must be performed at the system level, which will help identify security controls appropriate for that system. This publication discusses how an IoT device to be included as part of a larger system can be considered, which can impact those security controls, but does not solely dictate which controls are appropriate for the system, which must take into account 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 device 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 device doesn't store any data, it may not need to meet some data at rest requirements needed on other system elements. The IoT device 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 device affect magnitude(s) of impact 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." [CNSSI] The introduction of IoT devices into an information system can expand the harm to include human safety, environmental, and other impacts. IoT devices may introduce *greater*, *lower*, or *equal* magnitude of impact compared to the rest of the system. For example, an IoT device that is safety- and/or mission-critical may create *greater* magnitude of impact if compromised. A constrained IoT device (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 device, 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 device. Figure 6 shows how information about an IoT device will flow into the updated risk assessment of the system in which the IoT device 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 device, or that must be provided by the IoT device 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 device and/or other system elements.

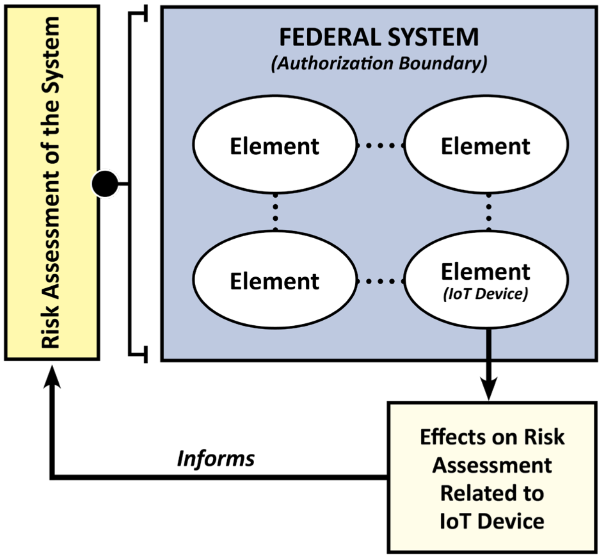


Figure 6: Effects on Risk Assessment due to IoT Device Informs the Risk Assessment of the Entire System.

3.3 Identifying Device Cybersecurity Requirements

Device 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 Section 3.1 and updates to the system risk assessment that may be necessary as discussed in Section 3.2. Figure 7 below illustrates this process and how it will draw on the considerations and guidance from the prior sections to inform the device cybersecurity requirements.

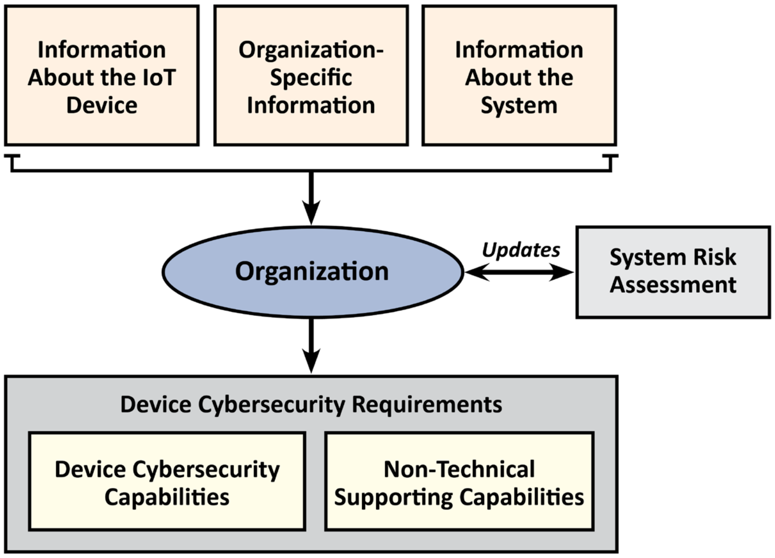

Information About the IoT Device
Organization-Specific Information
Information About the System
Organization
Updates
System Risk Assessment
Device Cybersecurity Requirements
Device Cybersecurity Capabilities
Non-Technical Supporting Capabilities

Figure 7: Organizations Can Gather Information to Update the System Risk Assessment and Determine Device Cybersecurity Requirements

Determining IoT device cybersecurity requirements may be challenging for some use cases. To assist organizations in selecting IoT device 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 device cybersecurity capabilities and non-technical supporting capabilities. Since IoT device cybersecurity requirements are in support of security controls allocated to information systems, organizations can identify the device cybersecurity requirements needed to support the security controls allocated to the information system(s) to which the IoT device will be connected. Information security and systems administration personnel should collaborate to identify security controls that require support from system elements (e.g., IoT devices).

Example of Device Cybersecurity Requirements Supporting Security Controls

An organization might want to acquire an IoT device 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 device 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 device 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 device 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 [800-213A]. This catalog contains device cybersecurity requirements organized by technical (i.e., device cybersecurity capabilities) and non-technical (i.e., non-technical supporting capabilities). The device cybersecurity requirements in the catalog are derived from security controls in SP 800-53 Rev. 5 and therefore may be helpful in supporting security controls in low, moderate, and high impact information systems.[22] SP 800-213A can be a valuable resource for organizations when identifying applicable IoT device cybersecurity requirements.

Organizations can use the mappings (i.e., between SP 800-53 Rev. 5 security controls and device cybersecurity requirements) included in SP 800-213A to identify appropriate device cybersecurity requirements. The mappings show, for each identified SP 800-53 Rev. 5 security control, the corresponding device 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 device cybersecurity capabilities and non-technical supporting capabilities. This list of device 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 device 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

[22] The device cybersecurity requirements (i.e., device 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.

organizationally-defined system use notification message or banner to be displayed on the IoT device." For many IoT devices and/or use cases, this capability is not applicable; organizations might choose to scope this identified capability out of the needed capabilities. Other identified device 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 device. If an organization is planning to acquire a constrained IoT device (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 device and those capabilities that will need to be provided by other system elements. Organizations should also carefully consider the key device cybersecurity requirements for an IoT device that *must* be present on the device for it to be integrated into the system.

3.3.2 Identifying Requirements using Other Resources

In addition to device cybersecurity capabilities and non-technical supporting capabilities identified using the mapping described in Section 3.3.1, organizations may determine that additional capabilities are needed from IoT devices 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.

Guidance that identifies applicable starting-points for device cybersecurity requirements may help some organizations overcome challenges they may encounter when determining appropriate device cybersecurity requirements for IoT devices. Organizations must hit a moving target in identifying device cybersecurity requirements to support a set of controls that may change based on the IoT device 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 specifies the high-level device technical cybersecurity capabilities that generally achieve minimal securability for most customers. The IoT core baseline, as the IoT device 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 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 [800-213A]. The federal profile uses the SP 800-53 Rev. 5 controls catalog [800-53] as an input source of federal government security needs and goals to identify device cybersecurity capabilities and non-technical supporting capabilities. Since the federal profile targets minimal securability for all federal government use cases, it focuses on device cybersecurity requirements that support the low-impact baseline set of SP 800-53 Rev. 5 controls, which would be a sub-set of the device 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 device cybersecurity requirements when incorporating an IoT device 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 device cybersecurity requirements for IoT devices. However, the federal profile and other lists of device cybersecurity requirements may not be a perfect fit for a specific IoT device, organization, and/or system. The list of device cybersecurity capabilities and non-technical supporting capabilities in the federal profile may still need to be tailored as described in Section 3.3.1[23]. In particular, the use of the low-impact baseline may not be appropriate for all organizations and use cases (e.g., if the IoT device is to be integrated into a moderate- or high-impact information system). Tailoring of device 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 device (e.g., having to procure another IoT device when the IoT device 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 device, prior to a purchase being made.

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

[23] Manufacturers may choose to incorporate the device cybersecurity requirements from the federal profile in their IoT devices, especially for IoT devices where federal agencies are an expected customer

4 Understanding Risk Management Options for IoT Devices

When preparing to acquire an IoT device, an organization may find that available IoT devices on the market do not provide some of the needed device cybersecurity requirements. Sometimes, organizations may also find that an IoT device lacks needed device cybersecurity requirements after purchasing the equipment. These situations, where the IoT device does not support all device cybersecurity requirements, do not necessarily preclude an organization from using the IoT device, but rather, indicates additional considerations are necessary to ensure appropriate use. In the same way that IoT devices 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 devices may affect appropriate risk mitigations.

Another important point is that an IoT device might still be securely used by an organization even if it doesn't provide all identified device cybersecurity requirements. In some use cases, the organization might determine that an identified device cybersecurity requirement is unnecessary for support of a control (e.g., if the IoT device 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 device justifiably (i.e., without introducing unacceptable risk) lacks the capabilities to support that security control. In another instance, the IoT device 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 device 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 device without introducing unacceptable risk due to gaps between identified device cybersecurity requirements and the device cybersecurity capabilities provided by IoT devices on the market.

An organization may still determine that certain device cybersecurity requirements cannot be missing from an IoT device (i.e., it is a *key* device cybersecurity requirement). Such a determination could preclude use of an IoT device 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 device. Section 4.1 will describe the discrete ways an IoT device may present challenges related to meeting device cybersecurity requirements. Section 4.2 follows on these challenges by discussing ways in which organizations, IoT devices, and/or their manufacturers and supporting third-party entities may be able to manage those challenges.

4.1 Potential Challenges Meeting Device Cybersecurity Requirements

Section 3 described how an organization can determine the necessary device cybersecurity requirements for an IoT device. When an organization attempts to acquire an IoT device, the identified device cybersecurity requirements can help guide the procurement process. Organizations can look for available IoT devices (and manufacturers) on the market that provide as many device cybersecurity requirements as possible within the target price point. Acquiring

[24] Alternative solutions for IoT may become more common (and cheaper) as IoT deployments increase and more customers are faced with similar risk mitigation challenges for which there are elegant and/or more efficient solutions for IoT.

IoT devices that provide more than just key device 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 device that goes beyond key device cybersecurity requirements may not be an option because locating IoT devices 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 devices. IoT devices may be intended for vastly different environments or uses, which can create variability in existence and efficacy of device cybersecurity requirements. In some cases, they may lack IoT device cybersecurity requirements because aspects of the use case interfere with the goal supported (e.g., for this device'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 device may be very broad, forcing a manufacturer to make choices about which capabilities to support in a device. The capabilities provided by the device may favor one customer's use case more than another customer's. This issue can be accentuated when an IoT device is being used by an *unintended* customer, who may find capabilities missing from the IoT device.
- The cost and complexity of providing capabilities in the IoT device may cause manufacturers to build fewer capabilities into devices. These decisions may reduce expectations for capabilities provided by the IoT device 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 device cybersecurity and non-technical supporting capabilities desired or delivered, which could sometimes be in conflict for a specific IoT device.

NISTIR 8228 Identifies IoT Device Cybersecurity Challenges

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

Gaps in support for device cybersecurity requirements may manifest from technological, form, cost, and other factors of the device that do not easily support or allow such capabilities, but gaps may exist even when there are not particular limitations on the device's capacity to achieve those requirements. For example, some IoT device manufacturers may simply not provide adequate documentation for a product and may be unresponsive to additional requests, or IoT devices may be technically able to support a device cybersecurity capability, but due to limited demand for such a capability, even from the federal government, the manufacturer may forgo or delay adding it. Legacy devices may also have gaps in device 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 device). For each device cybersecurity capability or non-technical supporting capability desired in an IoT device, there are three possible scenarios:

1. The device cybersecurity capability or non-technical supporting capability is present in the IoT device as the capability is stated.
2. The device 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 device 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 device, 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 device options, available solutions). These three device capability support scenarios can be valuable for communicating with a product vendor about where there may be gaps between the organization's desired device cybersecurity requirements and the capabilities provided by the IoT device[25].

4.2 Managing Gaps in IoT Device Cybersecurity Requirements

There may be reasons why an IoT device does not provide all the capabilities desired by a customer. Some amount of specialization in the design of IoT devices and their capabilities for organizations may be appropriate, but it is neither possible nor advisable for organizations to drive device cybersecurity capabilities into all IoT devices 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 device 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 device's cybersecurity capabilities may not be possible to accommodate. Some device cybersecurity capabilities may require a level of

[25] Other IoT ecosystem participants (e.g., vendors, manufacturers) may be aware of and support sets of device cybersecurity requirements, but these sets may not entirely align with an organization's expectations. For example, some IoT device manufacturers may use the Federal Profile of the IoT Device Cybersecurity Baselines to build towards in an attempt to meet as many federal customer's device cybersecurity requirements as they can suppose 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 device cybersecurity requirements. This set of capabilities, like any, is based on some number of assumptions about an IoT device, customer, and system that may not hold for the specific purchase. Clear understanding by an organization of which capabilities are present in and around the IoT device and how this compares to what is desired and expected will aid in overcoming challenges due to lack of support.

computing resources that is not supported by the IoT device. Changing such fundamental aspects of an IoT device (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 device cybersecurity requirements, including how to mitigate gaps between desired cybersecurity requirements and the capabilities provided by the IoT device. As organizations examine IoT devices available on the market, they shall determine which device cybersecurity requirements are provided by the IoT device (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 device:

1. Determine that the capability's support for the security control is justifiably missing from the IoT device 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 device/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 device's lack of support or alternative support for the security control is unacceptable.

As summarized in Figure 8, three of the four determinations mean an organization can likely integrate the device despite the gap in device cybersecurity capability. There are nuances to each determination that must be considered by organizations in deciding whether a specific device cybersecurity requirement gap means they can or cannot integrate the IoT device.

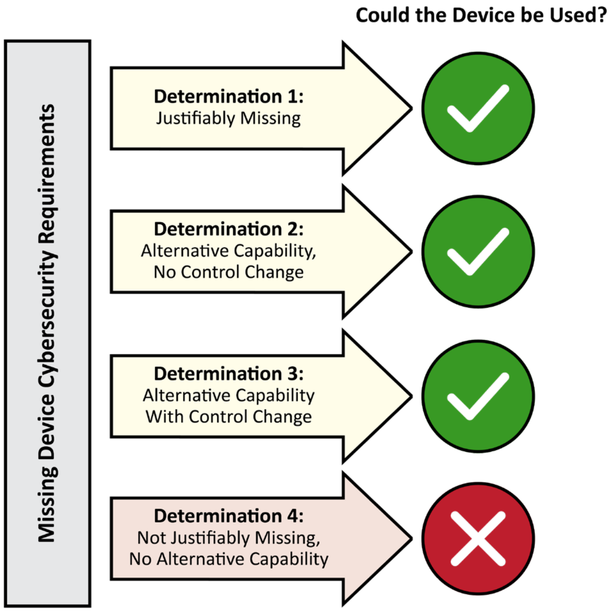

Could the Device be Used?
Missing Device Cybersecurity Requirements
Determination 1: Justifiably Missing
✓
Determination 2: Alternative Capability, No Control Change
✓
Determination 3: Alternative Capability With Control Change
✓
Determination 4: Not Justifiably Missing, No Alternative Capability
✗

Figure 8: Likely Outcomes for Organizations based on the Four Determinations Discussed

For the first determination, an organization acknowledges the lack of a device 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 device 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 device'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 device 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 device 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 device uses derived PIV credentials rather than PIV cards to authenticate a person's identity). The organization may determine that the IoT device'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 device 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 device, the device 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 device.

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

References

[500-292] 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

[800-18] 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

[800-30] 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

[800-37] 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

[800-39] Joint Task Force Transformation Initiative (2011) Manage 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

[800-40] Souppaya M, Scarfone K (2013) Guide to Enterprise Patch Management Technologies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 3. https://doi.org/10.6028/NIST.SP.800-40r3

[800-53] 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

[800-53B] 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

[800-56A] Barker E, Chen L, Roginsky A, Vassilev A, Davis R (2019) 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

[800-60] 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

[800-82] Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 2. https://doi.org/10.6028/NIST.SP.800-82r2

[800-128] Johnson A, Dempsey K, Ross R, 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. https://doi.org/10.6028/NIST.SP.800-128

[800-144] 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

[800-145] Mell P, 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

[800-146] Badger ML, Grance T, Patt-Corner R, Voas J (2011) 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

[800-160v1] Ross RS, Oren JC, McEvilley M (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018. https://doi.org/10.6028/NIST.SP.800-160v1

[800-160v2] Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R (2019) 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. https://doi.org/10.6028/NIST.SP.800-160v2

[800-161] Boyens J, Smith A, Bartol N, Winkler K, Holbrook A, Fallon M (2021) Cyber Supply Chain Risk Management Practices for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (SP) 800-161, Rev. 1. https://doi.org/10.6028/NIST.SP.800-161r1-draft

[800-213A] Fagan M, Marron, J, Brady KG, Jr, Cuthill BB, Megas KN, Herold R (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

[CNSSI] 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

[CSF] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

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

[IR8228] Boeckl K, Fagan M, Fisher W, Lefkovitz N, Megas K, Nadeau E, Piccarreta B, O'Rourke DG, Scarfone K (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

[IR8259] Fagan M, Megas KN, Scarfone K, Smith M (2020) Foundational Cybersecurity Activities for IoT Device Manufacturers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259. https://doi.org/10.6028/NIST.IR.8259

[IR8259A] Fagan M, Megas KN, Scarfone K, 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

[IR8259B] Fagan M, Marron J, Brady KG, Jr, Cuthill BB, Megas KN, Herold R (2020) 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

[IR8286] Stine K, Quinn S, Witte G, Gardner R (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. https://doi.org/10.6028/NIST.IR.8286

[ISO9000] International Organization for Standardization (2015) ISO 9000:2015 – Quality management systems – Fundamentals and vocabulary (ISO, Geneva, Switzerland).

[ISO15288] International Organization for Standardization (2015) ISO 15288:2015 – Systems and software engineering – System life cycle processes (ISO, Geneva, Switzerland).

[NICE] Petersen R, Santos D, Wetzel K, Smith M, Witte G (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

[SSDF] Dodson D, Souppaya M, Scarfone K (2020) Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper. https://doi.org/10.6028/NIST.CSWP.04232020

Appendix A—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
NISTIR	NIST Inter-agency or Internal Report
OMB	Office of Management and Budget
OT	Operational Technology
PIV	Personal Identity Verification
RMF	Risk Management Framework
SP	Special Publication

Appendix B—Glossary

Capabilities Catalog

Comprehensive list of device cybersecurity capabilities derived from analysis of comprehensive list of source documents for the application or sector. For the federal sector, NIST SP 800-53 Rev. 5 [800-53] provided the definition of controls used to create the NIST-generated capabilities catalog used for the Federal profile.

Configuration [800-128, Adapted]

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.

Core Baseline

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

Customer [ISO9000]

The organization or person that receives a product or service.

Device Cybersecurity Capability

Cybersecurity features or functions that computing devices provide through their own technical means (i.e., device hardware and software).

Device Cybersecurity Capability Core Baseline

See *core baseline*.

Device Identifier [800-56A, Adapted]

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).

Entity

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

Federal Profile

Profile of the IoT device cybersecurity capability core baseline [IR8259A] and non-technical supporting capability core baseline [IR8259B] to provide security guidance provided to federal government organizations related to IoT devices.

Interface [CNSSI, Adapted]

A boundary between the IoT device and entities where interactions take place. There are two types of interfaces: network and local.

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 Device Cybersecurity Requirement
A device cybersecurity requirement that if lacking from an IoT device (in the case of a device 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 [800-53, Adapted]
Computer programs and associated data that may be dynamically written or modified during the device's execution (e.g., application code, libraries).

Update [800-40, Adapted]
A patch, upgrade, or other modification to code that corrects security and/or functionality problems in software.