Draft NIST Special Publication 800-213

IoT Device Cybersecurity Guidance for the Federal Government:

Establishing IoT Device Cybersecurity Requirements

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

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

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

Draft NIST Special Publication 800-213

IoT Device Cybersecurity Guidance for the Federal Government:

Establishing IoT Device Cybersecurity Requirements

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

Rebecca Herold
The Privacy Professor
Des Moines, IA

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

December 2020

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

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

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, 30 pages (December 2020)
CODEN: NSPUE2

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

Public comment period: *December 15, 2020* through *February 26 ~~12~~, 2021*

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 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

Federal agencies 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 federal agencies consider how an IoT device they plan to acquire can integrate into a federal information 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 a federal agency 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 agencies better understand what kinds of device cybersecurity capabilities and supporting non-technical capabilities may be needed from or around IoT devices used by federal government agencies. To that end, NIST has developed a catalog (https://pages.nist.gov/IoT-Device-Cybersecurity-Requirement-Catalogs/) of IoT device cybersecurity capabilities and supporting non-technical capabilities for manufacturers and IoT device customers. This catalog identifies technical and non-technical capabilities that may be necessary for supporting NIST SP 800-53 controls implemented in federal information systems. Just as not every Federal IT system uses every control, not every capability in the catalog is needed in every IoT device. Ultimately, the goal is to enable federal agencies to securely incorporate IoT devices into their information systems and meet their security requirements.

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 Cybersecurity for IoT team members Brad Hoehn and Dave Lemire and the NIST FISMA Implementation Project team for their extensive help in copy editing.

Audience

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

Call for Patent Claims

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

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

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

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

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

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

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

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

Table of Contents

List of Appendices

List of Figures

1 Introduction

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

Existing NIST risk management guidance helps federal agencies satisfy their security requirements[3] from the information system level up through the organizational[4] 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 federal agencies will frequently be integrated as system elements, and this integration will often happen well after the information system has been initially deployed. As an example, an agency may purchase voice-activated printers and integrate them into the existing enterprise network. Agencies must also grapple with the challenge that many IoT devices lack features and functions that are common in conventional information technology (IT) equipment.

To help agencies 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 a federal agency 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 federal agencies 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,

[1] While the term *information systems* is used in the document. The scope of the document and concerns discussed would apply equally to operational technology (OT) systems.

[2] 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 and NISTIR 8259. NISTIR 8228 Section 2 provides additional detail on how device capabilities are understood relative to IoT devices.

[3] As identified in 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."

[4] Like other NIST guidance, *organization* is meant to describe entities of any size, complexity, or positioning within an organizational structure.

[5] A *system element* is 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. IoT devices will commonly be system elements relative to the federal information system they are connected to.

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 specific other devices (e.g., an IoT hub) or systems (e.g., a cloud) for some functionality[6]. While this publication might be helpful for IoT products 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) suite of security standards and guidance, address those situations more directly.

1.2 Target Audience

The target audience of this publication is information security professionals, system administrators, and others in federal agencies tasked with assessing, applying, and maintaining security on a federal information system. Personnel within the following Workforce Categories and Specialty Areas from the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [1] are most likely to find this publication of interest, as are their privacy counterparts:

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

1.3 Relationship to Other Publications

This publication uses concepts from the NIST Risk Management Framework, specifically publications such as NIST SPs 800-18 [2], 800-30 [3], 800-37 [4], 800-39 [5], 800-53 [6], 800-60 [7], 800-82[8], and 800-160 v1 [9] and v2 [10] as well as the NIST Cybersecurity Framework [11]. It also follows from the foundational cybersecurity for IoT work from NIST documented in NISTIR 8228 [12]and the NISTIR 8259 series [13, 14, 15, 16, 17]. 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, but as convention, security is used when discussing the protection of these for the system while cybersecurity is used when discussing how elements might support security or protect security themselves. This mixed terminology is motivated by 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.

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

1.4 Document Conventions

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

This document contains guidance for federal agencies when acquiring and/or integrating an IoT device into an existing information 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.

2 Background Considerations

This section presents background information about IoT devices that agencies should consider in their device acquisition processes. This publication draws from other NIST guidance, namely the Risk Management Framework (RMF) [4] and the Cybersecurity Framework (CSF) [11]. Since IoT devices will often be integrated into existing federal information systems, this publication will provide guidance for agencies 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; but systems are made up of elements. Increasingly, IoT devices may become elements of federal information systems. The relationship between systems and elements is a foundational concept in this publication. To understand more about this relationship between systems and elements, readers should refer to NIST Special Publication 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [4]. Some of the key concepts, particularly those covered in section 2.4 of SP 800-37, will be highlighted here. Figure 1 shows these concepts visually, adapted from a figure in SP 800-37, Revision 2.

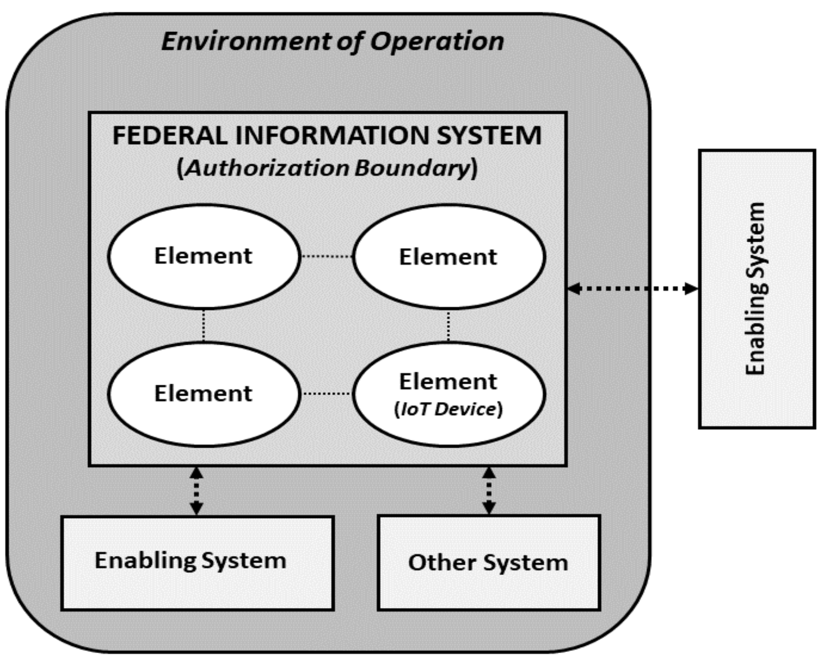

Figure 1 - Visualization of the System and Environment

An information system "is a set of interacting elements that are organized to achieve one or more stated purposes." [4] Information systems are defined by the authorization boundary, which for federal information systems will encapsulate elements owned and operated by federal agencies.

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 federal information system—as well as some enabling 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, federal agencies define and determine the parts of the environment of operation that are within the authorization boundary of each information system. As shown in Figure 1, 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, in general. Additional enabling systems will fall outside of the environment of operation (e.g., a system hosted by another agency or service provider). This concept of systems and elements can help clarify the ways IoT devices might be used by federal agencies and the subsequent identification of device cybersecurity requirements.

Some IoT devices might be best characterized as an other system if the IoT device is architected as a system that requires minimal interaction with the federal information system (e.g., the agency's internal network). An example of this type of other system might be a building or campus monitoring system that is primarily autonomous. Such an other system will mainly benefit from some of the federal information system's capabilities (e.g., an internet connection, access to data within the authorization boundary), while implementing its own security controls.

Other IoT devices acquired by federal agencies will be best characterized as system elements that fall within the authorization boundary of an existing information 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, agencies may have significantly more expectations about how this IoT device must support the security controls of the information system and/or organization. If the IoT device lacks technical and non-technical capabilities (discussed further in Section 2.2) to support the information system's security controls, challenges can arise for the agency. In this situation, the agency may need to implement compensating controls (e.g., creating a segmented network for IoT) or costly reimplementation of existing controls. If risk(s) introduced by the IoT device cannot be mitigated, the agency may have to 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 another system, or as an element of an existing system) but is primarily aimed at IoT devices as system elements since the agency typically has greater responsibility and control over these IoT devices. Understanding the IoT device's relationship to the information system is important to properly define the device cybersecurity requirements needed to support organizational and information system security requirements.

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 information system and organizational objectives. NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* [5], discusses how higher-level mission and organizational objectives inform the architecture and control structure around information systems. In this publication, we extend the discussion from SP 800-39, highlighting the connection between systems and elements as discussed in SP 800-37 and Section 2.1 above. Figure 2 shows the connection between the concepts discussed in SP 800-39 and system elements.

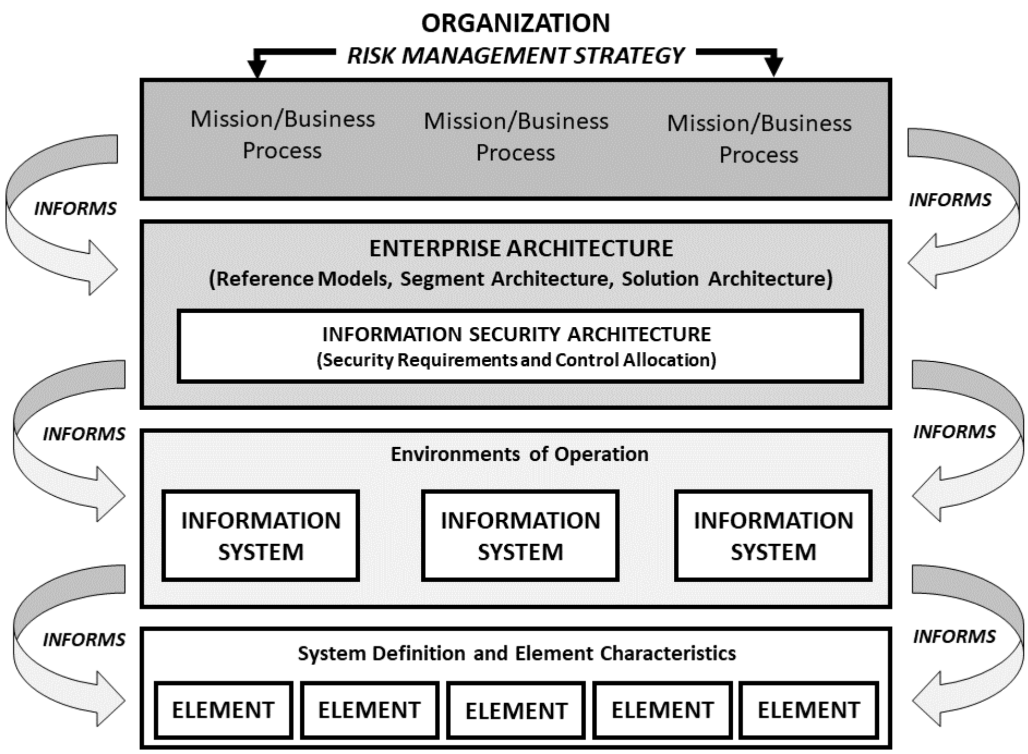

Figure 2 - Information Security Requirements Integration to the Element Level

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 information 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 information system and its security controls.

The primary way that IoT devices support security controls is via technical means, which are called *device cybersecurity capabilities*. 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 federal agencies. In particular, NISTIR 8259D, *Profile of the IoT Core Baseline for the Federal Government* [17], focuses on the federal government as a sector of IoT device customers and identifies foundational device cybersecurity capabilities needed in IoT devices acquired by the federal government. NISTIR 8259D also identifies *non-technical supporting capabilities*, which are actions that manufacturers or third parties take in support of the initial and on-going security of 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.

Both device cybersecurity capabilities and non-technical supporting capabilities are vital to federal agencies' ability to implement controls that the agency has allocated for their federal 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.

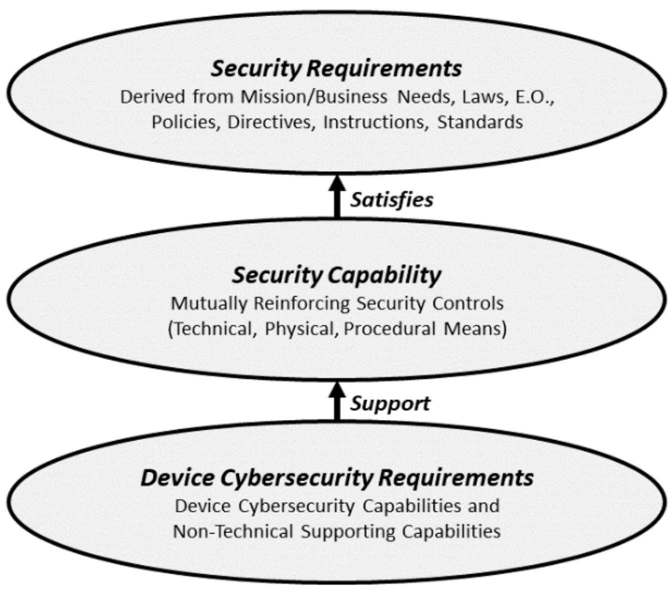

Figure 3 - Role of Device Cybersecurity and Non-Technical Supporting Capabilities in Satisfying Security Capabilities and Requirements

Allocation and application of security controls to information systems is a key step of risk management. Controls used by the federal government generally are selected from the NIST SP 800-53, Revision 5 *Security and Privacy Controls for Information Systems and Organizations* [6]. These controls are technology agnostic and can apply to IoT devices incorporated into federal information systems as system elements.

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 information system's risk assessment based on new risks introduced by the device. An altered risk assessment may require additional or new controls to be implemented in the information system.

The guidance in this publication focuses on establishing device cybersecurity requirements to support security controls. This publication does not provide details on how IoT devices may impact an information system's risk assessment or reallocation of controls that may be necessary. Readers are encouraged to reference SP 800-30, *Guide for Conducting Risk Assessments* 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 an information system can present a number of challenges for federal agencies. Federal agencies should strive to understand these challenges before an IoT device is integrated into an information system. For example, due to a number of market and technological factors, IoT devices often lack security functionality commonly present in conventional IT equipment (e.g., laptops). A lack of security functionality in an IoT device could introduce unacceptable levels of risk to the information system. NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* [12] details some of these challenges that IoT devices can create for federal agencies. The challenges described in NISTIR 8228 represent generic, high-level use cases. For specific agencies or particular IoT devices, the challenges faced could diverge from those explored in NISTIR 8228. Agencies 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).

Federal agencies 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* [9] demonstrates how an integrated process is best for engineering trustworthy systems. SP 800-160 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 considers acquisition early in system design and integration later, which are important concepts in building a trustworthy system. Federal agencies are encouraged to apply concepts from SP 800-160 when integrating IoT devices into information systems to ensure the trustworthiness of the information system.

Federal information systems will frequently be engineered at one point in time, but then modified as system elements are removed or other elements added. When IoT devices are added as system elements, federal agencies 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, a federal agency 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. Federal agencies 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 federal agencies in determining the applicable device cybersecurity requirements (i.e., the set of device cybersecurity capabilities and non-technical supporting capabilities) for an IoT device. Figure 4 illustrates the information sources that agencies can use to help identify device cybersecurity requirements. Each type of source is explored in more detail in this section.

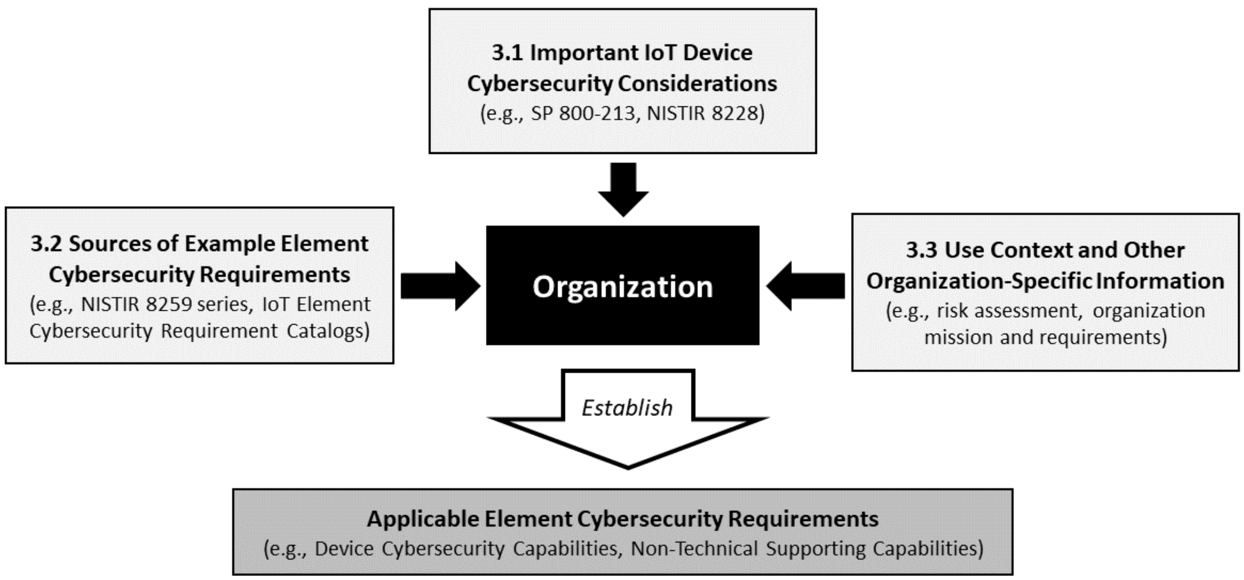

Figure 4 - Information Sources to Identify Device Cybersecurity Requirements

Section 3.1 provides an overview of important IoT device considerations. The questions in section 3.1 help federal agencies understand the device cybersecurity capabilities and non-technical supporting capabilities that are needed. Section 3.2 presents sources of device cybersecurity requirements. Federal agencies may reference these sources when selecting applicable IoT device cybersecurity requirements. Section 3.3 discusses how federal agencies can utilize organization-specific and information system-specific knowledge (e.g., controls allocated to the information system) to determine applicable device cybersecurity requirements.

Each federal agency should develop a process for identifying and articulating IoT device cybersecurity requirements that aligns with existing policies and procedures (e.g., acquisitions, security, system administrations, etc.). The guidance presented in this publication provides a starting point for agencies—as well as additional resources agencies can use—in identifying IoT device cybersecurity requirements.

3.1 Important IoT Device Cybersecurity Considerations

The decision to integrate an IoT device into a federal information system may occur for a variety of reasons (e.g., to achieve business objectives, further technical advancements, provide administrative support, etc.). The reason the IoT device is being acquired will influence its use case. For one agency, IoT sensors may be sought to help remotely monitor environmental conditions; another agency may acquire IoT office equipment to increase productivity; still other agencies may seek to leverage IoT technology in the delivery of services to citizens.

Agencies should fully understand the specific use case for an IoT device since the use case could influence device cybersecurity requirements. The following questions can help federal agencies think through some of the common considerations for IoT devices. The answers to these questions can ultimately help federal agencies identify IoT device cybersecurity requirements for their use case(s).

1. **What is the benefit of the IoT device and how will it be utilized?** Agencies 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, is the IoT device replacing equipment that did not connect to the information system? In such a case, agencies should consider the benefit of the system connection compared to the potential risks.

2. **What data is collected?** IoT devices can collect many kinds of data, some innocuous, others of concern to federal agencies. Any data collected could be a risk to the agency. All data collected or reported by IoT devices should be understood, but three main types of data may be of concern:

    1. *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.

    2. *Confidential agency/Federal government data:* The IoT device may collect agency restricted or confidential data. For example, IoT devices may help create or have access to agency-restricted test results, analysis materials, or device prototypes that require special protection.

    3. *Environmental data:* Many IoT devices can sense and/or collect data of, from, or about the physical environment. Federal agencies should consider whether the collection of environmental data poses any risk to individuals or the agency mission.

3. **In what technologies will the data be stored?** 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. Agencies 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), etc.

4. **In what geographic areas will the data be shared and/or stored?** The architecture that supports IoT devices is increasingly global. Federal agencies 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, federal agencies 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 a compromised IoT device could affect operations and the environment (e.g., alarms, thermostats, environmental controls, heating elements) as well as the security posture of the information 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 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 operational systems in federal agencies 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 hurt 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.
2. **Would the IoT device introduce unacceptable risks to the agency or result in non-compliance with cybersecurity requirements?** Organizations should also consider how they will secure the IoT device and mitigate any associated risks in accordance with their cybersecurity requirements. IoT devices can alter the level of impact (i.e., low, moderate, high) that has been determined for a system, which could, in turn, require additional controls. Some IoT devices might be unable to support the organization's current cybersecurity strategies due to their design, requiring agencies to implement compensating controls for the IoT device (e.g., network segmentation).
3. **Is the IoT device known to have had published 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. Federal agencies should look to these disclosures to inform themselves of known vulnerabilities. If the manufacturer cannot mitigate the vulnerabilities, agencies would have to identify and address risks introduced by the IoT device.

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 federal agencies if not adequately planned for. Federal agencies should refer to NISTIR 8228 and consider if the IoT device will create any security and privacy challenges for the information system and organization. Consider:

Are there aspects of the IoT device and its functionality that will cause foreseeable challenges when applying security controls? In particular, agencies should consider:

1. *Does the IoT device lack key device cybersecurity requirements?* Key device cybersecurity requirements are those the agency has determined that the IoT device must possess in order for the device to be integrated in the federal information system. Lack of key device cybersecurity requirements means that the IoT device cannot support existing information system controls and/or subsequently introduces unacceptable levels of risk to the information system.

2. *Will the implementation or maturity of device cybersecurity capabilities and/or non-technical supporting capabilities fail to satisfy the agency's key device cybersecurity requirements?* Some IoT devices may completely lack key device cybersecurity requirements, making the IoT device unusable by the federal agency. Other IoT devices may provide device cybersecurity requirements but not in the manner expected by the federal agency. For example, an IoT device may have a unique device identifier, but it may not be in a format the federal agency uses with other equipment. The agency 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, agencies may need to apply significant compensating controls.

By taking the time to carefully consider the preceding questions, agencies can understand, articulate the applicable IoT device cybersecurity requirements.

3.2 Sources of Device Cybersecurity Requirements

Determining IoT device cybersecurity requirements may be challenging for some use cases. To assist federal agencies in selecting IoT device cybersecurity requirements, this section presents several NIST publications. Federal agencies should reference these NIST publications to select IoT device cybersecurity requirements that support existing security controls as well as mitigate risks identified from the considerations in Section 3.1.

The NISTIR 8259 series of documents provides examples of device cybersecurity requirements as well as guidance that may be helpful to federal agencies. The NISTIR 8259 publications focus on helping manufacturers understand their critical role in the cybersecurity of IoT devices, which is rooted in the cybersecurity needs and goals of customers. This focus on the needs and goals of customers makes the 8259 series of documents helpful to organizations that are consumers of IoT devices.

NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers* [13], directs manufacturers to support the cybersecurity needs and goals of expected IoT device customers in the device's expected use case. The manufacturer's primary role is to ensure minimal securability, providing the minimum necessary device cybersecurity capabilities and non-technical supporting capabilities to meet customer needs and goals. NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline* [14] 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, *IoT Non-Technical Supporting Capability Core Baseline* [15] presents a set of non-technical supporting capabilities—the IoT non-technical supporting capability core baseline—generally needed from manufacturers or other third parties to support common cybersecurity 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., federal agency). NISTIR 8259C, *Creating a Profile Using the IoT Core Baseline and Non-technical Baseline* [16], discusses this process of profiling the IoT core baselines to identify IoT device requirements that best meet the customer's cybersecurity needs and goals.

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

Readers may be familiar with the low-, moderate-, and high-impact security control baselines in the NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*. The IoT core baselines are distinct from the SPP 800-53B security control baselines and shall be considered separately. 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.

NISTIR 8259D presents a profile of the IoT core baselines that is guided by the needs and goals of federal agencies. The federal profile in NISTIR 8259D uses the SP 800-53 controls catalog as an input source of federal government cybersecurity needs and goals. Whereas the controls in SP 800-53 generally focus on the information system and organization, the capabilities in the federal profile articulate the device cybersecurity capabilities and non-technical supporting capabilities needed to support the controls. The federal profile considers the IoT device as an information system element in which SP 800-53 security controls have already been identified and allocated.

Since the federal profile in NISTIR 8259D targets minimal securability for all federal government use cases, it focuses on device capabilities that support the low-impact baseline set of SP 800-53 controls. This focus is based on the assumption that the low-impact baseline set of controls—with minimal tailoring and application of compensating controls—will be used for many federal information systems. The federal profile in NISTIR 8259D is therefore recommended as a starting point for federal agencies to use when identifying IoT device cybersecurity requirements [7]. The use of the low-impact baseline will not be appropriate for all agencies and use cases, particularly if an IoT device is integrated into a moderate- or highimpact information system. The device cybersecurity requirements in the federal profile may not adequately support the security controls in moderate- and high-impact information systems.

In addition to the IoT core baselines and federal profile, federal agencies may also leverage the IoT Device Cybersecurity Requirement Catalogs [https://pages.nist.gov/IoT-Device-Cybersecurity-Requirement-Catalogs/]. These two catalogs contain additional 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 catalogs are derived from security controls in SP 800-53 and therefore may be helpful in supporting security controls in moderate and high impact information systems. The NIST Pages Catalogs can be a valuable resource for federal agencies when identifying applicable IoT device cybersecurity requirements.

Federal agencies shall identify all applicable IoT device cybersecurity requirements, ensuring that information system security controls are supported while also incorporating output from the considerations in Section 3.1. Federal agencies in communicating these device cybersecurity requirements to manufacturers, will need to consider how to consolidate requirements with those of other federal organizations to effectively achieve economies of scale. If the IoT device and/or manufacturer will not provide all required device cybersecurity capabilities and non-technical supporting capabilities, agencies should follow established risk management strategies to plan for the IoT device's incorporation into the information system.

3.3 Use Context and Other Organization-Specific Information

The guidance in Sections 3.1 and 3.2 will aid federal agencies in identifying applicable IoT device cybersecurity requirements. Device cybersecurity requirements should be based on the security capabilities and security requirements of the information system and organization. For this reason, the set of device cybersecurity requirements identified through the guidance in Sections 3.1 and 3.2 should be tailored according to the use context and other organization-specific information.

Since IoT device cybersecurity requirements are in support of security controls allocated to information systems, federal agencies 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).

Federal agencies 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

[7] 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

devices that may help federal agencies determine the risk associated with an IoT device. It is important for federal agencies to identify all security controls required for an information system before identifying the device cybersecurity requirements to support those controls. This is especially important if additional security controls (or increased support for existing controls) are needed. All applicable security controls should be considered when selecting device cybersecurity requirements. Ideally the inclusion of an IoT device as a new system element will not significantly alter the information system's risk assessment. Following this process will help federal agencies avoid purchase of unusable devices or unintended introduction of unmitigated risks.

Example of Device Cybersecurity Requirements Supporting Security Controls

An agency 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 federal information system (e.g., internal network) so that agency management can remotely (but within the environment of operation) access 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 federal agency 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.

When the full set of security controls is identified, federal agencies can translate those controls into device cybersecurity capabilities and non-technical supporting capabilities. Information security and systems administration personnel could leverage their expertise about security controls to identify appropriate device cybersecurity requirements from the NIST Pages Catalogs, the federal profile, and other profiles/lists of device cybersecurity requirements. Agency personnel can also leverage existing mappings between device cybersecurity requirements and SP 800-53 controls. These mappings are located in the NIST Pages Catalogs.

Organization-specific Considerations Impact Device Cybersecurity Requirements

When selecting IoT device cybersecurity requirements, agencies also need to consider how organization-specific policies, procedures, or environment may affect device cybersecurity requirements. In the previous call-out box, an example was presented of a smart speaker that requires proper authentication and authorization before allowing connections. Does the agency require Personal Identity Verification (PIV) card-based authentication or does it allow password-based authentication in limited circumstances? These agency policies will influence IoT device cybersecurity requirements. Does the agency purchase products from particular manufacturers or 3rd parties? The IoT devices available to the agency through those parties may limit the device cybersecurity capabilities and non-technical supporting capabilities available. Are there any environmental considerations (e.g., temperature, humidity, etc.) in the environment of operation? If so, device requirements may need to account for these environmental considerations. These organization-specific considerations may impact not only the device cybersecurity requirements, but also the design of the device. In the examples above, perhaps the IoT device needs to provide support for derived PIV credentials, or the IoT device may need to have a durable housing to withstand excessive heat while still providing functionality. Agencies will need to carefully account for these organizational considerations that may impact device requirements.

697 # References

[1] 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

[2] Swanson M, 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 https://doi.org/10.6028/NIST.SP.800-18r1

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

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

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

[6] 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. https://doi.org/10.6028/NIST.SP.800-53r5

[7] 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

[8] 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

[9] 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

[10] 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

[11] 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

[12] Boeckl K, Fagan M, Fisher W, Lefkovitz N, Megas K, Nadeau E, Piccarreta B, O'Rourke DG, Scarfone K (2018) 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

[13] 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

[14] 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

[15] 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), Draft NIST Interagency or Internal Report (IR) 8259B. https://doi.org/10.6028/NIST.IR.8259B-draft

[16] Fagan M, Marron, J, Brady KG, Jr, Cuthill BB, Megas KN, Herold R (2020) Creating a Profile Using the IoT Core Baseline and non-technical baseline. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Interagency or Internal Report (IR) 8259C. https://doi.org/10.6028/NIST.IR.8259C-draft

[17] Fagan M, Marron, J, Brady KG, Jr, Cuthill BB, Megas KN, Herold R (2020) Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259D. https://doi.org/10.6028/NIST.IR.8259D-draft

[18] Cyber-Physical Systems Public Working Group (2017) Framework for Cyber-Physical Systems: Volume 1, Overview, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1500-201. https://doi.org/10.6028/NIST.SP.1500-201

[19] 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

[20] 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

[21] 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

[22] 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

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

Appendix A—Acronyms

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

CSF	Cybersecurity Framework
FISMA	Federal Information Security Modernization Act
IoT	Internet of Things
ITL	Information Technical Laboratory
LTE	Long-term Evolution
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OT	Operational Technology
RMF	Risk Management Framework
SP	Special Publication
UWB	Ultrawide Band

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 *Security and Privacy Controls for Information Systems and Organizations* provided the definition of controls used to generate the NIST generated capabilities catalog used for the Federal profile.
Configuration [19, 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 [23]	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 [20, 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 [14] and non-technical supporting capability core baseline [15] to provide security guidance provided to federal government organizations related to IoT devices.
Interface [21, 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).
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 [6, Adapted]	Computer programs and associated data that may be dynamically written or modified during the device's execution (e.g., application code, libraries).
Update [22, Adapted]	A patch, upgrade, or other modification to code that corrects security and/or functionality problems in software.