NIST Special Publication 800-213A

IoT Device Cybersecurity Guidance for the Federal Government:

IoT Device Cybersecurity Requirement Catalog

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

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

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

NIST Special Publication 800-213A

IoT Device Cybersecurity Guidance for the Federal Government:

IoT Device Cybersecurity Requirement Catalog

Michael Fagan
Katerina N. Megas
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
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.800-213A

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 800-213A
Natl. Inst. Stand. Technol. Spec. Publ. 800-213A, 94 pages (November 2021)
CODEN: NSPUE2

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

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

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

This publication provides a catalog of internet of things (IoT) device cybersecurity capabilities (i.e., features and functions needed from a device to support security controls) and non-technical supporting capabilities (i.e., actions and support needed from device manufacturers and other supporting entities to support security controls) that can help organizations as they use Special Publication (SP) 800-213 to determine and establish device cybersecurity requirements. This catalog cross references the capabilities in the catalog to the cybersecurity controls in NIST SP 800-53. Organizations should refer to SP 800-213 as that publication provides necessary context to effectively use this catalog and related material.

Keywords

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

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 federal organizations tasked with assessing, applying, and maintaining security on a federal information 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

1 Introduction

1.1 Purpose and Applicability

This publication is intended to help federal organizations determine device cybersecurity requirements for IoT devices they seek to use with federal information systems and other systems operated by the federal government.[1] 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 specific other devices (e.g., an IoT hub) or systems (e.g., a cloud) for some functionality[2].

This publication shall be used with the guidance in Special Publication (SP) 800-213, *IoT Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements* [800-213] [3]. Federal organizations can use this catalog of device cybersecurity requirements to determine those appropriate to support the security controls implemented on their system and in their organization. *Device cybersecurity requirements* are *device cybersecurity capabilities* and *non-technical supporting capabilities* needed to integrate an IoT device into a system. Device cybersecurity capabilities are cybersecurity features or functions that computing devices provide through their own technical means (i.e., device hardware and software). For example, data protection using encryption would be a *device cybersecurity capability* if implemented on an IoT device. Non-technical supporting capabilities are actions an organization (i.e., manufacturers of IoT devices or designated third-party entities with a supporting role) performs in support of the cybersecurity of an IoT device. For example, notifications when an update is available and training of how to apply the software update may be a *non-technical supporting capability* needed by a federal organization in support of the cybersecurity of an IoT device.

This catalog provides a resource for federal organizations to use in determining and describing device cybersecurity requirements needed to support security in their information systems and organization. When used with the guidance in SP 800-213 and the NIST Risk Management Framework (RMF), [4] this catalog can help increase the security posture of systems and elements.

---

[1] IoT devices naturally bring many connections to a system through its actuation and networking capabilities. Any *system* that includes as a system element an IoT device 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 or align with the system of interest.

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

[3] The catalog in this publication should be used in the context of the process described in SP 800-213 [800-213]. This includes, but is not limited to, understanding and considering the impact an IoT device may have on the security controls allocated for a system and organization (i.e., through a risk reassessment) before determining requirements.

[4] NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, describes the Risk Management Framework (RMF) and provides guidelines for applying the RMF to information systems and organizations [800-37].

1.2 Target Audience

The target audience of this publication is information security professionals, system administrators, procurement professionals, and others in federal organizations 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) Workforce Framework for Cybersecurity [NICE] are most likely to find this publication of interest:

- 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 directly relates to SP 800-213 [800-213]. 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]. Direct mappings and references to SP 800-53 [800-53] are also used in the catalog to show the connection between device cybersecurity requirements and security controls a federal organization may be using.

1.4 Publication Organization

The rest of this publication contains the catalog of device cybersecurity requirements divided into two sections:

- Section 2 details seven device cybersecurity capabilities and several related sub-capabilities that may be needed from an IoT device to support system security controls.
- Section 3 details four non-technical supporting capabilities and several related sub-capabilities that may be needed from IoT device manufacturers and supporting entities.

Each section of device cybersecurity requirements provides the name, description, and additional informative discussion for each capability and sub-capability. Many sub-capabilities have additional information in the form of individual *requirements* that may be part of the device cybersecurity requirement. Each sub-capability includes a mapping to applicable SP 800-53 controls. Figure 1 shows the structure of a capability and sub-capability.

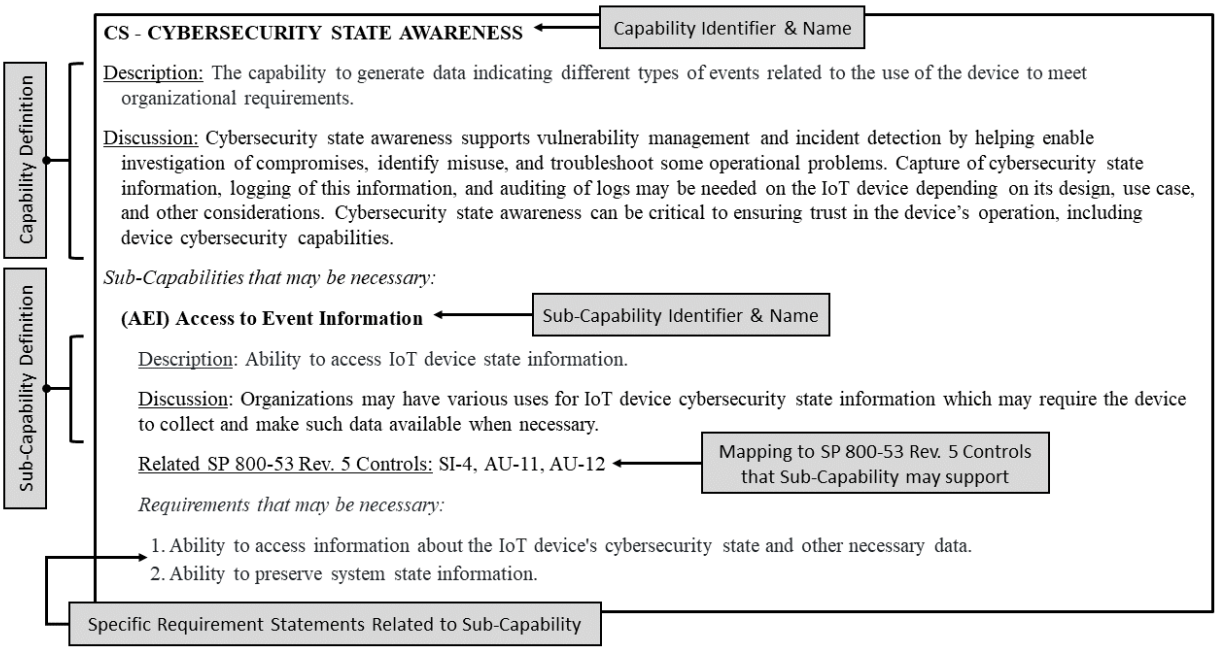

Figure 1: Capability and Sub-Capability Structure

[5] and then defined with a short description accompanied by further discussion about the nature of and need for the capability overall. These high-level descriptions can help organizations identify which capabilities they should consider in support of system and organizational security controls. In this context of SP 800-213, a capability is further defined by the sub-capabilities that describe the details of device cybersecurity requirements.

For each capability, this catalog also documents sub-capabilities that describe distinct, more specific details to further define support needed related to the higher-level capability. The need for a sub-capability or its elements is guided by the cybersecurity needs of the organization as described in SP 800-213. Figure 1 shows the structure of a sub-capability, which like capabilities are named and defined with a short description and further discussion about the sub-capability and why it may be needed.

[5] Capability names follow from NISTIRs 8259A [IR8259A] and 8259B [IR8259B], which were used as inputs along with SP 800-53 Rev. 5 [800-53] to generate this catalog.

A mapping to related SP 800-53 Rev. 5 controls is also provided for each sub-capability that can help organizations identify the controls and/or enhancements[6] that may be supported by each sub-capability. This support for controls may come from a fulfilment of all or part of a control by the presence of the functionality or actions described in the sub-capability. For example, the control may state that the element should function in a specific way and the sub-capability describes how the IoT device should function based on the control. In other cases, support for controls is in the form of enabling the system and/or organization to perform some system/organization-wide function or action including the IoT device. Controls are considered independent of their inclusion in SP 800-53B, *Control Baselines for Information Systems and Organizations* [800-53B], and so some controls included in the related controls list may not be in the low-, moderate-, and/or high-impact baseline. As explored in SP 800-213 [800-213], these mappings are meant to be used with a prior understanding of security controls to the system to which the IoT device will connect and selection of device cybersecurity requirements guided by that understanding. The mappings do not imply that each mapped security control is necessary in the presence of the sub-capability.

Finally, many sub-capabilities contain individual requirements that can be used by the organization to provide additional detail to a device cybersecurity requirement based on their applicability.

Using Catalog Content Identifiers

Throughout this catalog, each capability and sub-capability are given identifiers that's allow to shorter identification of specific content. For example, the Cybersecurity State Awareness sub-capability Access to Event Information shown in Figure 1 could be referred to as CS:AEI. Additionally, the numbered *requirements that may be necessary* can be referred to using those numeral (e.g., CS:AEI(1) or CS:AEI(2)). Finally, some *requirements that may be necessary* have another level below that are labeled using alphabetic characters (i.e., a, b, c), which can also be incorporated into this shorthand (e.g., DO:SMP(1a) or DO:SMP(2a,b)). This notation is used in Appendices B and C.

[6] Organizations should note that applicable control enhancements are sometimes included in the mapping for a sub-capability without the corresponding control that would be assumed in place if the enhancement is in place. Mappings in this catalog reflect the controls and/or enhancements from SP 800-53 Rev. 5 [800-53] that may be supported by the functionality or actions described in the sub-capability. In some cases, control enhancements are supported by the sub-capability while the base control may not be since enhancements represent an augmentation of the base control, which could require additional, distinct support from system elements like IoT devices.

2 Device Cybersecurity Capability Catalog

A device cybersecurity capability is a feature or function that computing devices (i.e., an IoT device) provides through its own technical means (i.e., device hardware and software) [800-213]. Organizations will many times need device cybersecurity capabilities to be present in system elements, including IoT devices, that directly or indirectly implement and support security controls. This section identifies device cybersecurity capabilities and sub-capabilities organizations should consider when establishing device cybersecurity requirements. The device cybersecurity capabilities identified are:

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

DI - DEVICE IDENTIFICATION

Description: The capability to identify the IoT device for multiple purposes and in multiple ways to meet organizational requirements.

Discussion: Device identification supports many cybersecurity needs and goals, such as asset management, vulnerability management, access management, data protection, and incident detection. The unique logical identifier can be used to distinguish the device from all others, usually for automated device management and monitoring. Multiple identifiers may be necessary for an organization, each possibly to be used together or for individual purposes. For example, an IoT device may support both a way to identify it uniquely on the system or Internet as well as a way to identify its expected device behavior (e.g., using a Manufacturer Usage Description (MUD) URL).

Sub-Capabilities that may be necessary:

(IMS) Identifier Management Support

Description: Ability for device identification.

Discussion: The ability to identify system elements is important to asset management and monitoring of the system, fundamental tasks in applying many other security controls. IoT devices being delivered with a unique identifier for use by the organization may be necessary for the IoT device to conform to the organization's security controls.

Related SP 800-53 Rev. 5 Controls: IA-3, IA-4

Requirements that may be necessary:

1. Ability to uniquely identify the IoT device logically.
2. Ability to uniquely identify a remote IoT device.
3. Ability for the device to support a unique device identifier (e.g., to allow it to be linked to the person or process assigned to use the IoT device).

(AID) Actions Based on Device Identity

Description: Ability to perform actions that can occur based on or using the identity of the device.

Discussion: Using IoT device identifiers to perform additional actions can help provide assurance security controls are applied to all applicable system elements by allowing for differentiation between devices and more thorough accounting of the application of security controls to system elements.

Related SP 800-53 Rev. 5 Controls: AU-2, CM-8, CM-8(8), IA-3, AC-3, SI-4

Requirements that may be necessary:

1. Ability to configure IoT device access control policies using IoT device identity.
    a. Ability to hide IoT device identity from non-authorized entities.
    b. Ability for the IoT device to differentiate between authorized and unauthorized remote users.
    c. Ability for the IoT device to differentiate between authorized and unauthorized physical device users (e.g., using a method of authentication to verify the identity of physical device users).
2. Ability to monitor specific actions based on the IoT device identity.
3. Ability to identify software loaded on the IoT device based on IoT device identity.
4. Ability for the device identifier to be used to discover the IoT device for the purpose of network asset identification and management.

(DAS) Device Authentication Support

Description: Ability to support local or interfaced device authentication.

Discussion: The IoT device may need to have the ability to authenticate its identity with other system elements (e.g., other IT and IoT devices) and likewise authenticate the identity of those system elements.

Related SP 800-53 Rev. 5 Controls: IA-3

Requirements that may be necessary:

1. Ability for the IoT device to identify itself as an authorized entity to other devices.
2. Ability to verify the identity of other devices.

(PID) Physical Identifiers

Description: Ability to add a unique physical identifier at an external or internal location on the device authorized entities can access.

Discussion: Identifying system elements via physical identifiers allow for asset management to be performed or checked using the physical means, sometimes in addition and in coordination with logical means.

Related SP 800-53 Rev. 5 Controls: IA-3

DC - DEVICE CONFIGURATION

Description: The capability to configure the IoT device through logical and/or physical interfaces to meet organizational requirements.

Discussion: Device configuration supports vulnerability management, access management, data protection, and incident detection. Organizations may want to alter a device's configuration for a variety of reasons (e.g., cybersecurity, interoperability, privacy, and usability). Without a device configuration capability, an organization cannot customize a device to meet its specific needs and may not be able to securely integrate the device into the authorized entity's environment. Many other cybersecurity capabilities will have or require a configuration capability to allow proper use of the features and functions by the organization. Protection and management of configuration data may be necessary to ensure the confidentiality, integrity, and availability of the configurations.

Sub-Capabilities that may be necessary:

(PRV) Logical Access Privilege Configuration

Description: Ability for only authorized entities (e.g., organization personnel, other system elements, enabling systems) to apply logical access privilege settings within the IoT device and configure logical access privilege as described in Logical Access to Interfaces.

Discussion: Access privileges in an access control environment is critical to ensuring the system can limit access to information as dictated by policy and privilege level. Limiting configuration of such privileges to authorized entities helps ensure the integrity of access privileges.

Related SP 800-53 Rev. 5 Controls: AC-3, CM-5

(AUT) Authentication and Authorization Configuration

Description: Ability for only authorized entities to configure IoT device authentication policies and limitations as described in Logical Access to Interfaces.

Discussion: Aspects of the authentication mechanisms and system policies for authentication may need to be configured by the organization. It is critical that changes to such configurations be limited to authorized entities to ensure integrity of authentication.

Related SP 800-53 Rev. 5 Controls: AC-3, CM-5

(INT) Interface Configuration

Description: Ability for only authorized entities to configure aspects related to the device's interfaces as described in Logical Access to Interfaces.

Discussion: Organizations may need to configure interfaces based on their organizational characteristics. Changes to interface configurations should be limited to authorized entities

to protect the integrity of those configurations.

Related SP 800-53 Rev. 5 Controls: AC-3, CM-5

(DSP) Display Configuration

Description: Ability to configure content to be displayed on a device.

Discussion: Based on the use case, IoT devices may need to display, or restrict display of, specific content to meet security controls and requirements (e.g., notices of use of a federal computer system).

Related SP 800-53 Rev. 5 Controls: AC-8, AC-12(2), AC-12(3)

(CTL) Device Configuration Control

Description: Ability to change configurations on the IoT device based on operational events as described in Device Security and Cybersecurity Event Awareness.

Discussion: Various aspects of the IoT device and how it operates may need to be configured by the organization to ensure conformance and support for security controls. Some additional aspects may also be necessary, such as the ability to restore the configuration to a secure state.

Related SP 800-53 Rev. 5 Controls: CM-2, CM-3, CM-5, CM-6, SR-11(2)

Requirements that may be necessary:

1. Ability for authorized entities to change the device's software configuration settings.
2. Ability for authorized entities to restore the device to a secure configuration defined by an authorized entity.
3. Ability to maintain control over device configuration during service and repair.
4. Configuration settings for use with the Device Configuration capability including, but not limited to:
    a. Ability for authorized entities to configure the cryptography use itself, such as choosing a key length.
    b. Ability for authorized entities to configure any remote update mechanisms to be either automatically or manually initiated for update downloads and installations.
    c. Ability for authorized entities to enable or disable notification when an update is available and specify who or what is to be notified.
    d. Ability for authorized entities to configure authentication mechanisms (e.g., minimum password length or complexity, force change of passwords on first use)

DP - DATA PROTECTION

Description: The capability to protect IoT device data to meet organizational requirements.

Discussion: Data protection on an IoT device supports cybersecurity needs and goals such as access management, system and organizational data protection, and incident detection. Confidentiality , availability, and integrity of data is central to cybersecurity. Privacy protections may also need to be specifically considered for certain use cases. Many times, data protection is implemented using cryptographic modules and functions. NIST has significant guidance around these areas through the Federal Information Processing Standards (FIPS) [NIST FIPS] and Cryptographic Module Validation Program [CMVP], and readers are referred to these publications, programs, and projects for more information about appropriate cryptographic modules for IoT data protection.

Sub-Capabilities that may be necessary:

(CRY) Cryptography Capabilities and Support

Description: Ability for the IoT device to use cryptography for data protection.

Discussion: Use of acceptable cryptographic modules and functions to ensure confidentiality and integrity, and avoid undermining availability of information is common in systems and among system elements. Organizations should refer to FIPS 140-3 [FIPS-140], 180-4 [FIPS-180], 186-4 [FIPS-186], 197 [FIPS-197], 198-1 [FIPS-198], and 202 [FIPS-202] for more information about Federal Information Processing Standards for cryptographic modules and functions.

Related SP 800-53 Rev. 5 Controls: SC-13, SC-17

Requirements that may be necessary:

1. Ability to execute cryptographic mechanisms of appropriate strength and performance.
2. Ability to obtain and validate certificates.
3. Ability to verify digital signatures.
4. Ability to run hashing algorithms (i.e., compute and compare hashes).
5. Ability to perform authenticated encryption algorithms.

(KEY) Cryptographic Key Management

Description: Ability to manage cryptographic keys securely.

Discussion: (Under construction)

Related SP 800-53 Rev. 5 Controls: SA-9(6), SC-12, SC-12(6), SC-13

Requirements that may be necessary:

1. Ability to manage cryptographic keys securely:
   a. Ability to generate key pairs.
   b. Ability to store encryption keys securely.
   c. Ability to change keys securely.
   d. Ability to maintain exclusive control of cryptographic keys when used by external systems.

(STO) Secure Storage

Description: Ability for the IoT device, or tools used through the IoT device interface, to enable secure device storage.

Discussion: Many IoT devices will store some data for some period of time, and so proper protection of that data may be necessary using acceptable cryptographic modules. Other aspects of how the IoT devices stores and handles data, such as the ability to securely erase data stored in the device, may be part of this sub-capability's elements since these may also be necessary to ensure compliance with security controls.

Related SP 800-53 Rev. 5 Controls: CP-9, CP-9(8), MP-6, SC-28

Requirements that may be necessary:

1. Ability to support encryption of data at rest.
   a. Ability to cryptographically store passwords at rest, as well as device identity and other authentication data.
   b. Ability to support data encryption and signing to prevent data from being altered in device storage.
2. Ability to secure data in device storage.
   a. Ability to secure data stored locally on the device.
   b. Ability to secure data stored in remote storage areas (e.g., cloud, server, etc.).
   c. Ability to utilize separate storage partitions for system and user data.
3. Ability to securely back-up the data on the IoT device.
4. Ability to "sanitize" or "purge" specific or all data in the device.

(STX) Secure Transmission

Description: Ability to secure data transmissions sent to and from the IoT device.

Discussion: Protection of data as it is transmitted to and from the device using acceptable cryptographic modules may require support from the IoT device (e.g., by encrypting/decrypting data that is sent/received). This sub-capability can help ensure confidentiality and integrity of transmitted data.

Related SP 800-53 Rev. 5 Controls: SC-8(1)

Requirements that may be necessary:

1. Ability to configure the cryptographic algorithm to protect data in transit.
    a. Ability to support trusted data exchange with a specified minimum strength cryptography algorithm.
    b. Ability to support data encryption and signing to prevent data from being altered in transit.
2. Ability to utilize one or more capabilities to protect the data it transmits from unauthorized access and modification.
3. Ability to use cryptographic means to validate the integrity of data transmitted.
4. Ability to use organization-internal normalized formats to protect the data it transmits.

LA - LOGICAL ACCESS TO INTERFACES

Description: Ability to require authentication to, and/or identification of, the IoT device, and to establish authentication and identification configuration and display requirements.

Discussion: The logical access to interfaces capability supports cybersecurity needs and goals such as vulnerability management, access management, data protection, and incident detection. The ability to access the device will support its management and use for cybersecurity. Some form factors or use cases may vary in the kinds of interfaces available for accessing the device (e.g., if a physical screen is not possible). A key aspect of this capability is the ability for organizations to control access to interfaces. Limiting access to interfaces reduces the attack surface of the device, giving attackers fewer opportunities to compromise it. For example, unrestricted network access to an IoT device enables attackers to directly interact with the device, which significantly increases the likelihood of the device being compromised. Authentication of other entities (e.g., humans, other devices) will be a common way to support logical access to interfaces, which has been addressed in FIPS 201-2 [FIPS-201] and SP 800-63 [800-63].

Sub-Capabilities that may be necessary:

(AUN) Authentication Support

Description: Ability to support authentication methods.

Discussion: To control logical access to interfaces, the IoT device may need to support adequate authentication methods. Some IoT devices or organizations may need support for Personal Identity Verification (PIV). More information about PIV can be found in FIPS 201-2 [FIPS-201].

Related SP 800-53 Rev. 5 Controls: AC-17(10), IA-2, IA-2(1), IA-2(2), IA-6

Requirements that may be necessary:

1. Ability for the IoT device to require authentication prior to connecting to the device, including using remote access.
2. Ability for the IoT device to support and require appropriate authentication.
3. Ability for the IoT device to support a second, or more, authentication method(s) through an out of band path such as:
    a. Temporary passwords or other one-use logon credentials
    b. Third-party credential checks
    c. Biometrics
    d. Text messages
    e. Hard Tokens
    f. Other methods
4. Ability for the IoT device to hide or mask authentication information during authentication process.

5. Ability to use federated authentication technologies (e.g., SAML, OAuth2, or Active Directory/Azure Active Directory).

(ACF) Authentication Configuration

Description: Ability to require, or not require, authentication to, and/or identification of, the IoT device, and to establish authentication and identification configuration and display requirements.

Discussion: Organizations may need to configure aspects of the authentication mechanism present in the IoT device to conform with access control security requirements. This sub-capability can support application of organizational policies around access privilege management, such as the management of access accounts and privileges of those accounts.

Related SP 800-53 Rev. 5 Controls: AC-2(2), AC-2(3), AC-2(5), AC-3(8), AC-7, AC-9, AC-17, AU-2, IA-8

Requirements that may be necessary:

1. Ability to set and change authentication configurations, policies and limitations settings for the IoT device.
    a. Ability to set the time period for how long the device will remain locked after an established configurable limit of unsuccessful login attempts has been met.
    b. Ability to disable or lock access to the device after an established number of unsuccessful login attempts.
    c. Ability to display and/or report the previous date and time of the last successful login authentication.
    d. Ability to automatically disable accounts for the IoT device after an established period of inactivity.
        i. Ability to support automatic logout of inactive accounts after a configurable established time period.
        ii. Ability to support automatic removal of temporary, emergency and other special use accounts after an established time period.
    e. Ability to report or log failed login attempts.
2. Ability to authenticate external users and systems.
3. Ability to revoke the access of accounts and/or external users and systems.

(USE) System Use Notification Support

Description: Ability to support system use notifications.

Discussion: Some IoT devices may have to alert users that the IoT device uses a federal information system and provide notices consistent with federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Some organizations may require the ability for an IoT device to display such notices in order to comply with their security requirements.

Related SP 800-53 Rev. 5 Controls: AC-8

Requirements that may be necessary:

1. Ability to display to IoT device users an organizationally-defined system use notification message or banner prior to successful IoT device authentication. (e.g., the message or banner would provide privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance).
2. Ability to create an organizationally-defined system use notification message or banner to be displayed on the IoT device.
    a. Ability to edit an existing IoT device display.
    b. Ability to establish the maximum size (in characters, bytes, etc.) of the available device display.
3. Ability to keep the notification message or banner on the device screen until the device user actively acknowledges and agrees to the usage conditions.

(AUZ) Authorization Support

Description: Ability to restrict all unauthorized interactions.

Discussion: Limitation of actions and interactions possible based on privileges associated with an authenticated identity is important to controlling interface access.

Related SP 800-53 Rev. 5 Controls: IA-2

Requirements that may be necessary:

1. Ability to identify authorized users and processes (e.g., applications).
2. Ability to differentiate between authorized and unauthorized users (physical and remote).

(AIM) Authentication & Identity Management

Description: Ability to establish access to the IoT device to perform organizationally-defined user actions without identification or authentication.

Discussion: Organizations may need certain actions performed on or with the device accessible without identification or authentication to meet organizational needs. The actions may be defined by the use case or other aspects of how the organization plans to use the IoT device.

Related SP 800-53 Rev. 5 Controls: AC-14

(ROL) Role Support & Management

Description: Ability to establish unique, privileged, organization-wide, and other types of

IoT device user accounts.

Discussion: Some IoT devices may have multiple users within an organization and require support for role and account management. These accounts may then be used are part of the identification, authentication, and authorization of users based on roles and privileges.

Related SP 800-53 Rev. 5 Controls: AC-2, AC-2(1), AC-2(7), AC-2(8), AC-2(9), AC-3, AC-3(7), AC-3(12) AC-6, AC-21, IA-4, SC-2

Requirements that may be necessary:

1. Ability to create unique IoT device user accounts.
2. Ability to assign roles to IoT device user accounts.
3. Ability to identify unique IoT device user accounts.
4. Ability to support a hierarchy of logical access privileges for the IoT device based on roles (e.g., admin, emergency, user, local, temporary, etc.).
    a. Ability to establish user accounts to support role-based logical access privileges.
    b. Ability to administer user accounts to support role-based logical access privileges.
    c. Ability to use organizationally-defined roles to define each user account's access and permitted device actions.
    d. Ability to support multiple levels of user/process account functionality and roles for the IoT device.
5. Ability to apply least privilege to user accounts (i.e., to ensure that the processes operate at privilege levels no higher than necessary to accomplish required functions).
    a. Ability to create additional processes, roles (e.g., admin, emergency, temporary, etc.) and accounts as necessary to achieve least privilege.
    b. Ability to apply least privilege settings within the device (i.e., to ensure that the processes or applications operate at privilege levels no higher than necessary to accomplish required functions).
    c. Ability to limit access to privileged device settings that are used to establish and administer authorization requirements.
    d. Ability for authorized users to access privileged settings.
6. Ability to support organizationally-defined actions for the IoT device.
    a. Ability to create organizationally-defined accounts that support privileged roles with automated expiration conditions.
    b. Ability to establish organizationally-defined user actions for accessing the IoT device and/or device interface.
    c. Ability to enable automation and reporting of account management activities.
    d. Ability to assign access to IoT device audit controls to specific roles or organizationally-defined personnel.
    e. Ability to control access to IoT device audit data.

f. Ability to identify the user, process or device requesting access to the audit/accountability information (i.e., to ensure only authorized users and/or devices have access).
g. Ability to establish conditions for shared/group accounts on the IoT device.
h. Ability to administer conditions for shared/group accounts on the IoT device.
i. Ability to restrict the use of shared/group accounts on the IoT device according to organizationally-defined conditions.

7. Ability to implement dynamic access control approaches (e.g., service-oriented architectures) that rely on:
   a. run-time access control decisions facilitated by dynamic privilege management.
   b. organizationally-defined actions to access/use device.
8. Ability to allow information sharing capabilities based upon the type and/or role of user attempting to share the information.
9. Ability to restrict access to IoT device software, hardware, and data based on user account roles, used with proper authentication of the identity of the user to determine type of authorization.

(LDU) Limitations on Device Usage

Description: Ability to establish restrictions for how the device can be used.

Discussion: Aspects of how the IoT device can be used by internal and external users may have to be limited by the organization to comply with security and organizational requirements. In some instances, limitations may have to apply to all who interact with the device, but in others the limitation may change based on various factors.

Related SP 800-53 Rev. 5 Controls: AC-10, AC-21(2)

Requirements that may be necessary:

1. Ability to establish pre-defined restrictions for information searches within the device.
2. Ability to establish limits on authorized concurrent device sessions for:
   a. User accounts
   b. Roles
   c. Groups
   d. Dates
   e. Times
   f. Locations
   g. Manufacturer established parameters

(XCN) External Connections

Description: Ability to support external connections.

Discussion: Complexities of how system resources are distributed and managed by organizations may require them to securely make external connections to comply with and support security controls.

Related SP 800-53 Rev. 5 Controls: AC-10, AC-20(1), AC-21, SC-8

Requirements that may be necessary:

1. Ability to securely interact with authorized external, third-party systems.
2. Ability to allow for the user/organization to establish the circumstances for when information sharing from the device and/or through the device interface will be allowed and prohibited.
3. Ability to establish automated information sharing to approved identified parties/entities.
4. Ability to identify when the external system meets the required security requirements for a connection.
5. Ability to establish secure communications with internal systems when the device is operating on external networks.

(IFC) Interface Control

Description: Ability to establish controls for the connections made to the IoT device.

Discussion: Many aspects of how the IoT device can be interacted with may have to be controlled by the organization to comply with security controls, but which will depend on the organization, system, and IoT device.

Related SP 800-53 Rev. 5 Controls: AC-3, AC-6, AC-17, AC-17(4), AC-18, CM-5, CM-7, SI-15

Requirements that may be necessary:

1. Ability to establish requirements for remote access to the IoT device and/or IoT device interface including:
    a. Usage restrictions
    b. Configuration requirements
    c. Connection requirements
    d. Manufacturer established requirement
2. Ability to restrict use of IoT device components (e.g., ports, functions, microphones, video).

3. Ability to logically or physically disable any local and network interfaces that are not necessary for the core functionality of the device.
4. Ability to restrict updating actions to authorized entities.
5. Ability to restrict access to the cybersecurity state indicator to authorized entities.
6. Ability to restrict use of IoT device services.
7. Ability to enforce the established local and remote access requirements.
8. Ability to prevent external access to the IoT device management interface.
9. Ability to control the IoT device's logical interface (e.g., locally or remotely).
10. Ability to change IoT device logical interface(s).
11. Ability to control device responses to device input.
12. Ability to control output from the device.
13. Ability to support wireless technologies needed by the organization (e.g., Microwave, Packet radio (UHF/VHF), Bluetooth, Manufacturer defined)
14. Ability to support communications technologies (including but not limited to):
    a. IEEE 802.11
    b. Bluetooth
    c. Ethernet
    d. Manufacturer defined
15. Ability to establish and configure IoT device settings for wireless technologies including authentication protocols (e.g., EAP/TLS, PEAP).

SU - SOFTWARE UPDATE

Description: Ability to update IoT device software, and to have support mechanisms for such updates.

Discussion: Software update is central to vulnerability management by allowing for software to be changed when vulnerabilities are found and remediated. Correcting IoT device operational problems with software updates can improve device availability, reliability, performance, and other aspects of device operation. Aspects of the software update capability may be dictated by the form factor, use case, organization, or security controls. For example, some IoT devices may have limited physical access, making remote updating more practical. Some organizations may want a rollback capability in the event that an update inadvertently impacts critical applications or integration with other systems, while other organizations may prefer to eliminate the risk of someone intentionally or inadvertently rolling software back to a vulnerable version.

Sub-Capabilities that may be necessary:

(UPD) Update Capabilities

Description: Ability to update the IoT device software within the device and/or through the IoT device interface.

Discussion: This sub-capability describes how an IoT device's update capability should function regarding the application of the update and parameters of the application. Organizations may need to identify specific requirements for the update mechanism to ensure it can be effectively used within the broader vulnerability and patch management policies they implement.

Related SP 800-53 Rev. 5 Controls: AU-1, CM-3, CM-5, CM-14, SI-7(15)

Requirements that may be necessary:

1. Ability to update the software by authorized entities only using a secure and configurable mechanism.
2. Ability to identify the current version of the organizational audit policies and procedures governing the software update.
3. Ability for authorized entities to roll back updated software to a previous version (i.e., uninstall an update)
4. Ability to restrict software installations to only authorized individuals or processes.
5. Ability to restrict software changes/uninstallations and other software update actions to only authorized individuals or processes.
6. Ability to verify software updates come from valid sources using an effective method (e.g., digital signatures, checksums, certificate validation, etc.).

7. Ability to execute the software update mechanism with fault tolerance such that a failed or interrupted update (e.g., loss of communication while downloading, device power loss while installing) does not degrade the IoT device's cybersecurity state.

(APP) Update Application Support

Description: Ability to update the device's software through remote (e.g., network download) and/or local (e.g., removable media) means

Discussion: Organizations may need to identify specific requirements for how updates are delivered to ensure they can be effectively monitored within the broader vulnerability and patch management policies they implement. Some IoT devices may also tie application of an update with its delivery (e.g., in an automatic update mechanism), which organization may consider as part of their identification of device cybersecurity requirements.

Related SP 800-53 Rev. 5 Controls: SI-2

Requirements that may be necessary:

1. If software updates are delivered and applied automatically:
    a. Ability to verify and authenticate any update before installing it
    b. Ability to enable or disable updating
2. If software updates are remote:
    a. Ability to set update mechanisms functions (e.g., download, installation) to be either automatically or manually initiated.
3. If notifications for software updates are delivered through the IoT device:
    a. Ability to enable or disable notification when an update is available
    b. Ability to specify which entities should receive notifications

CS - CYBERSECURITY STATE AWARENESS

Description: The capability to generate data indicating different types of events related to the use of the device to meet organizational requirements.

Discussion: Cybersecurity state awareness supports vulnerability management and incident detection by helping enable investigation of compromises, identify misuse, and troubleshoot some operational problems. Capture of cybersecurity state information, logging of this information, and auditing of logs may be needed on the IoT device depending on its design, use case, and other considerations. Cybersecurity state awareness can be critical to ensuring trust in the device's operation, including device cybersecurity capabilities.

Sub-Capabilities that may be necessary:

(AEI) Access to Event Information

Description: Ability to access IoT device state information.

Discussion: Organizations may have various uses for IoT device cybersecurity state information which may require the device to collect and make such data available when necessary.

Related SP 800-53 Rev. 5 Controls: AU-11, AU-12, SI-4

Requirements that may be necessary:

1. Ability to access information about the IoT device's cybersecurity state and other necessary data.
2. Ability to preserve system state information.

(EIM) Event Identification & Monitoring

Description: Ability to provide event identification and monitoring capabilities and/or support event identification and monitoring tools interfacing with the device.

Discussion: Monitoring for cybersecurity and other adverse events is a component of many organizations' control set to enable proactive assessment of cybersecurity posture. IoT devices may have to support this kind of monitoring, and the nature of the monitoring (e.g., events or channels of interest) may be related to the IoT device's use case.

Related SP 800-53 Rev. 5 Controls: AU-2, AU-13, CA-7, CM-3, CM-6, IA-2, SC-7, SC-15, SC-42, SI-4

Requirements that may be necessary:

1. Ability to identify organizationally-defined cybersecurity events (e.g., expected state change) that may occur on or involving the IoT device.

2. Ability to monitor for organizationally-defined cybersecurity events (e.g., expected state change) that may occur on or involving the IoT device.
3. Ability to support a list of events that are necessary for auditing purposes (to support the organizational auditing policy).
4. Ability to identify unique users interacting with the device (to allow for user session monitoring).
5. Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. (The device may be able to perform this check itself or provide the information necessary for an external process to check).
6. Ability to monitor communications traffic.
7. Ability to monitor changes to the configuration settings.
8. Ability to detect remote activation attempts.
9. Ability to detect remote activation of a collaborative computing device/component (e.g., microphone, camera).
10. Ability to detect remote activation of sensors.
11. Ability to define the characteristics of unapproved content.
12. Ability to scan files for unapproved content.

(EVR) Event Response

Description: Ability for the device to respond to organizationally-defined cybersecurity events in an organizationally-defined way.

Discussion: Further action after detection of a cybersecurity event may be necessary as part of an organization's event monitoring controls. IoT devices may have to conform with these requirements and contain features or functions that help it respond to cybersecurity events as the organization needs.

Related SP 800-53 Rev. 5 Controls: AU-5, AU-6, CP-13, IR-4, RA-7, SC-15, SC-42, SI-4

Requirements that may be necessary:

1. Ability to generate alerts for specific events.
2. Ability to respond to alerts according to predefined responses.
3. Ability to alert connected information systems of potential issues found during the auditing process.
4. Ability to provide information to an external process that will issue auditing process alerts.
5. Ability to notify users of activation of a collaborative computing device.
6. Ability to provide a physical indicator of sensor use.
7. Ability to respond following an auditing failure (either by the device or an external auditing process).
8. Ability to prevent download of unapproved content.

9. Ability to delete unapproved content.
10. Ability to support alternative security mechanisms when primary mechanisms (e.g., login protocol, encryption, etc.) are compromised.
11. Ability to configure organizationally-defined aspects of the event response.

(LCT) Logging Capture & Trigger Support

Description: Ability for the device, or an interfaced system, to generate, store, retain, delete, and report on specific device audit events, to run specific audit checks, and report findings in a variety of ways.

Discussion: Logs and audit of those logs may be important to how an organization implements and verifies security controls. IoT devices may have to support specific logging and audit practices as required by the organization.

Related SP 800-53 Rev. 5 Controls: AU-2, AU-3

Requirements that may be necessary:

1. The device can generate audit logs for defined events
    a. Ability to identify and capture organizationally-defined events using a persistent method.
    b. Ability to capture information from organizationally-defined cybersecurity events (e.g., cybersecurity state, time) through organizationally-defined means (e.g., logs).
    c. Ability to create audit logs within the device for organizationally-defined and auditable events (e.g. account creation, modification, enabling, disabling, removal actions and notifications).

(RDL) Support of Required Data Logging

Description: Ability for the device to capture required information in audit logs.

Discussion: The IoT device may have to capture and log certain data required by the organization. The kind of data captured and how it should be stored will be related to aspects of how the device functions, how the organization uses the device, how the organization handles data logging, among other considerations.

Related SP 800-53 Rev. 5 Controls: AU-2, AU-3, AU-4, AU-5(1), AU-5(5), AU-11

Requirements that may be necessary:

1. Ability to track users interacting with the device, the time they interacted with the device, the time the user logged out of the device, and to list this information in an audit log.
2. Ability to log information pertaining to:

   a. The type of event that occurred.
   b. The time that the event occurred.
   c. Where the event occurred.
   d. The source of the event.
   e. The outcome of the event.
   f. Identity of users/processes associated with the event.
3. Ability to support auditing of configuration actions such as:
   a. Current configuration state.
   b. History of configuration changes.
   c. When changes in configuration occurred.
   d. Which account made the configuration change.
4. Ability to provide information as to why the device captured a particular event or set of events.
5. Ability to capture organizationally-defined information to support examination of security incidents.
6. Ability to record stored data access and usage.
7. Ability to use an alternative audit logging mechanism in case of failure of primary mechanism.

(LSR) Audit Log Storage & Retention

Description: Ability to maintain audit logs in accordance with organizational policy.

Discussion: Once captured, there may be additional requirements from the organization dictating the retention and maintenance of the logs for some amount of time after they are created.

Related SP 800-53 Rev. 5 Controls: AU-4, AU-5(1), AU-11

Requirements that may be necessary:

1. Ability to comply with organizational policy for storing persistent audit logs up to a predefined size.
2. Ability to comply with organizational policy for audit log retention period.
3. Ability to delete audit logs in accordance with organizational policy.
4. Ability to send alerts that the logs are too big for the device to continue to store (if the predefined amount of time has not yet passed to delete them).

(SRT) Support for Reliable Time

Description: Ability to use timestamps to record the time an auditing event occurred.

Discussion: When logging with time-based information (e.g., a timestamp), having reliable timekeeping is critical to allowing for effective use of the logs when audited. Use of

common timekeeping mechanisms (e.g., network time) will suffice for some IoT devices, but other deployments and use cases may require alternative methods to provide reliable time.

Related SP 800-53 Rev. 5 Controls: AU-2, AU-8, SC-45(1)

Requirements that may be necessary:

1. Ability to support organizationally-defined granularity in device timing measurements.
2. Ability to use synchronization with a verified time source to determine the validity of a timestamp.
3. Ability to record timestamps convertible to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) to support a standardized representation of timing.
4. Ability to log timing measurements outside a threshold value (e.g., enabling alerts if the device's system time is not reliable).

(AUP) Audit Support & Protection

Description: Ability for the device to support and protect audit activities and associated data.

Discussion: Organizations will need to use logged information as part of audits to implement security controls and comply with requirements. IoT devices may have to support through features and functions some aspects of that audit process, such as providing access to or transmitting logs when needed by the organization.

Related SP 800-53 Rev. 5 Controls: AU-5(5), AU-6, AU-7, AU-9, SI-4

Requirements that may be necessary:

1. Ability to report on its cybersecurity state.
2. Ability to support a self-audit generation process.
3. Ability to run audit scans (automated or otherwise) to provide specific information (e.g., such as that requested for an external process to audit the device).
4. Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow for review, analysis, and reporting).
5. Ability to support an alternate auditing process in the event that the primary auditing process fails.
6. Ability to protect the audit information through the use of:
    a. Encryption.
    b. Digitally signing audit files.
    c. Securely sending audit files to another device.
    d. Other protections created by the device manufacturer.

7. Ability to prevent any entities from editing audit logs unless the entity is authorized and is responsible for maintaining the audit logs.

(AWR) State Awareness Support

Description: Ability to differentiate between when a device will likely operate as expected from when it may be in a degraded cybersecurity state.

Discussion: Fundamentally, the goal of cybersecurity state awareness is to make an organization able to know when a device will operate as expected and when it will not. For some IoT devices and use cases, logging may not be the most effective or only way this is achieved, and other features and functions may be needed by organizations to effectively monitor cybersecurity state on the IoT device and across the system. In other cases, IoT devices may have to self-assess their state to a limited extent to help ensure secure execution.

Related SP 800-53 Rev. 5 Controls: SA-8(21), SI-6

DS - DEVICE SECURITY

Description: The capability to secure the IoT device to meet organizational requirements.

Discussion: Some device cybersecurity requirements may dictate aspects of the IoT device's operation that do not fit cleanly into the other six device cybersecurity capabilities, but are nonetheless technical features or functions implemented in the device's hardware and software. This device security capability helps place those kinds of requirements in a broad context of device cybersecurity requirements. Many of the sub-capabilities in this capability support several other device cybersecurity capabilities by providing additional confidence in the implementation or execution of the other capabilities.

Sub-Capabilities that may be necessary:

(EXE) Secure Execution

Description: Ability to protect the execution of code on the device.

Discussion: Some IoT devices may need additional assurances of the secure execution of code to ensure confidentiality, integrity, and availability of the IoT device, its functionality, and its data. Many factors, such as the criticality and use case of the IoT device may impact the need and elements of this sub-capability.

Related SP 800-53 Rev. 5 Controls: SC-2, SC-39

Requirements that may be necessary:

1. Ability to enforce organizationally-defined execution policies.
    a. Ability to execute code in confined virtual environments.
    b. Ability to separate IoT device processes into separate execution domains.
2. Ability to separate the levels of IoT device user functionality.
3. Ability to authorize various levels of IoT device functionality.

(COM) Secure Communication

Description: Ability to securely initiate and terminate communications with other devices.

Discussion: Proper use of communications channels by IoT devices can help reduce the introduction and exploit of vulnerabilities, but also ensures availability of the IoT device to the organization and system as part of operations. Federal organizations may need to detail how they expect IoT devices to establish and terminate network connections.

Related SP 800-53 Rev. 5 Controls: SC-7, SC-7(17), SC-8, SC-10, SC-11, SC-16(2), SC-21, SC-23, SC-51, SI-10(6), SI-14(3)

Requirements that may be necessary:

1. Ability to enforce traffic flow policies.
2. Ability to utilize standardized protocols.
3. Ability to establish network connections.
4. Ability to terminate network connections (e.g., automatically based on organizationally-defined parameters).
5. Ability to de-allocate Transmission Control Protocol/Internet Protocol (TCP/IP) address/port pairings.
6. Ability to establish communications channels.
7. Ability to secure the communications channels.
8. Ability to interface with Domain Name System/Domain Name System Security Extensions (DNS/DNSSEC).
9. Ability to store and process session identifiers.
10. Ability to identify and track sessions with identifiers.
11. Ability to use an anti-spoofing mechanism to prevent adversaries from falsifying security attributes.
12. Ability to prevent untrusted data injections.

(RSC) Secure Resource Usage

Description: Ability to securely utilize system resources and memory.

Discussion: Vulnerabilities can arise from many places, including misuse of legitimate device resources and components. Safeguards on computing resources and memory can help reduce these kinds of vulnerabilities and may be needed by federal organizations as part of security controls.

Related SP 800-53 Rev. 5 Controls: CP-12, SC-4, SC-5, SC-24, SC-34, SC-39, SC-51, SI-17

Requirements that may be necessary:

1. Ability to support shared system resources.
    a. Ability to release resources back to the system.
    b. Ability to separate user and process resources use.
2. Ability to manage memory address space assigned to processes.
3. Ability to enforce access to memory space through the kernel.
4. Ability to prevent a process from accessing memory space of another process.
5. Ability to enforce configured disk quotas.
6. Ability to continue operation when associated networks are unavailable (e.g., a smart smoke detector must still go off when a fire occurs even if it is not attached to the associated network).

7. Ability to provide sufficient resources to store and run the operating environment (e.g., operating systems, firmware, applications).
8. Ability to utilize file compression technologies (e.g., to provide denial of service protection).
9. Ability to use or enforce hardware-based, write protect to protect certain software (e.g., firmware).

(DIN) Device Integrity

Description: Ability to protect against unauthorized changes to hardware and software.

Discussion: Ensuring the continued integrity of the IoT device's hardware and software components can help avoid introduction or exploit of vulnerabilities. Federal organizations may vary in the device integrity requirements, and those requirements may further vary based on aspects of how the IoT device is used by the organizations (e.g., criticality of the device, risk associated with its use).

Related SP 800-53 Rev. 5 Controls: CA-9(1), CM-8(3), SC-34, SR-9, SR-9(1)

Requirements that may be necessary:

1. Ability to perform security compliance checks on system components (e.g., verify acceptable baseline configuration, perform a tamper check).
2. Ability to detect unauthorized hardware and software components and other tampering with the IoT device when used.
3. Ability to detect tampering throughout the system development lifecycle.
4. Ability to take organizationally-defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a USB port is present).
5. Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).

(ONB) Secure Network Onboarding Support

Description: Ability to use secure network onboarding technologies to connect to the network.

Discussion: Organizations may use secure onboarding technologies on the network that facilitates communication for the system the IoT device is connecting to. This sub-capability identifies the necessary features and functions from the IoT device to support secure network onboarding.

Related SP 800-53 Rev. 5 Controls: IA-5, SC-7, SC-16

Requirements that may be necessary:

1. Ability for the IoT device to provide necessary data and/or perform necessary functions participate in the device-to-network authentication.
2. Ability to identify and recognize the network.
3. Ability to receive, store, and/or use secure network credentials.
4. Ability to restrict communications to only authorized entities, as enforced through the onboarded network.

(OPS) Secure Device Operation

Description: Ability to operate securely and safely.

Discussion: Federal organizations may need various internal safe-guards on the IoT device to support secure use on their system and within their organization. This sub-capability may also be necessary to increase efficacy or resiliency of existing capabilities or controls.

Related SP 800-53 Rev. 5 Controls: CM-2(7), CM-7, CP-10, CP-12, IR-4(5), PE-10, PE-12, PE-13, PE-14, PE-15, SC-24, SC-45, SC-45(1), SI-6

Requirements that may be necessary:

1. Ability to keep an accurate internal system time.
2. Ability to compare and synchronize internal system time with an organizationally-defined authoritative source.
3. Ability to define various operational states.
4. Ability to support various modes of IoT device operation with more restrictive operational states.
    a. "travel mode" for transit.
    b. "safe mode" for operation when some or all network security is unavailable.
    c. Others as determined necessary based on the purpose and goals for the IoT device.
5. Ability to define differing failure types.
6. Ability to fail in a secure state.
7. Ability to disable operations and/or functionality in the event of security violations.
8. Ability to restrict components/features of the IoT device (e.g., ports, functions, protocols, services, etc.) in accordance with organizationally-defined policies.
9. Ability to sense the environment and securely (i.e., preserving confidentiality, integrity, and availability of the device and its data) interface with the environment, either directly or through the IoT system. Examples include:
    a. Emergency shutoff mechanism
    b. Emergency lighting mechanism
    c. Fire protection mechanism
    d. Temperature and humidity mechanism

e. Water damage protection mechanism
f. Manufacturer defined capability

3 Non-Technical Supporting Capability Catalog

Non-technical supporting capabilities are defined as actions an organization (i.e., manufacturers and supporting entities) performs in support of the cybersecurity of an IoT device [800-213]. Organizations integrating IoT devices into their systems may need information or other kinds of support from other organizations, such as the IoT device manufacturer or other supporting entity to implement and ensure compliance with security controls. This section identifies non-technical supporting capabilities and sub-capabilities organizations should consider when establishing IoT device cybersecurity requirements. The non-technical supporting capabilities identified are:

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

DO - DOCUMENTATION

Description: The ability for the manufacturer and/or the manufacturer's supporting entity, to create, gather, disseminate, and store information relevant to cybersecurity of the IoT device prior to customer purchase, and throughout the development of a device and its subsequent lifecycle.

Discussion: Documentation of cybersecurity information helps potential IoT device customers to make informed purchase decisions that support their organization's cybersecurity requirements for IoT devices and/or systems where they are used. Documentation of important cybersecurity information also then helps enable secure use of the IoT device by customers after the purchase since it serves as the source of information for customers. Documentation is also important to support legal requirements (regulatory, contractual, web site security and privacy policies, etc.), for audits or other certifications that some customers may require for the IoT devices they use, and/or to support due diligence activities. Documentation about maintenance requirements, especially regarding the supporting entities contracted by the manufacturer to perform maintenance, device changes, and other activities, also supports the customer's need to adequately plan for maintenance activities.

Sub-Capabilities that may be necessary:

(SMP) Assumptions Made in Product Development

Description: Document assumptions made during the development process and other expectations related to the IoT device.

Discussion: This documentation will provide important information to customers describing the additional actions that may be needed based upon the assumptions and expectations the manufacturer has for their customers.

Related SP 800-53 Rev. 5 Controls: AC-1, AC-3, AC-3(7), AC-14, AT-3, AU-1, AU-9, IA-1, IA-2(1), MA-1, PE-3, PE-6, PM-3, PM-20, PL-1, PS-6, PT-4(1), PT-5, SI-1, SI-4, SI-7, SI-12, SI-21, SR-3, SR-5

Requirements that may be necessary:

1. Establish communications describing the IoT device security, authorization, and supporting maintenance requirements. To support these needs, manufacturers are encouraged to include details and actions such as:
    a. Providing details for the device security capabilities, along with how to implement the security management and operational controls, and supporting maintenance activities, for the IoT device.
    b. Providing details about the types of, and situations that trigger, local and/or remote maintenance activities required once the device is purchased and deployed in the organization's digital ecosystem.

c. Describing the ability to establish management roles to perform specified information security activities, and to establish security requirements, for the IoT device.
d. Establishing and providing communications that describe the suggested types of resources necessary to protect the associated information system(s) within which the IoT device will be deployed.
e. Providing details about the IoT device data security and privacy capabilities and limitations, and the types of risks mitigated by the capabilities.
f. Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.
g. Providing other information and actions as necessary for physically securing, and securely using, the IoT device based upon the IoT device use, purpose, and other contextual factors related to the digital ecosystem(s) within which they are intended to be used.

2. Establish communications describing options for implementing security oversight of IoT device users connected to the network. To support these needs, include details and actions such as:
    a. Providing descriptions of the types of physical access practices, and manufacturer suggested hardware or other types of devices, that can be used to prevent unauthorized physical access to the IoT device based upon the determined risk level that the device brings to the IoT customer's system.
    b. Providing descriptions of the physical access security procedures the manufacturer recommends to limit physical access to the device, and to associated device controls.
    c. Providing details of indications, and recommendations for how to determine, when unauthorized physical access to the IoT device was or is attempted, or is occurring.
3. Establish communications explaining how to accomplish logical organizational oversight for using the IoT device. Information that may be necessary to provide to explain how to accomplish logical oversight of the IoT device include details and actions such as:
    a. Providing information to IoT device customers with recommendations or suggestions for implementing management and operational controls.
    b. Providing IoT device customers the tools, assistance, instructions, and other types of information to support establishing a hierarchy of role-based privileges within the IoT device.
    c. Providing recommendations to IoT device customers for using the technical IoT device security controls, or external devices or applications

communicating with the IoT device, to establish a variety of oversight capabilities for the IoT device users.

4. Establish communications that describe the ways in which the IoT device can logically access devices on the FIPS-201 approved products list[7]. Information that may be necessary to provide include details and actions such as:
    a. Providing information and details to the IoT device customers indicating if and when the IoT device was placed on the FIPS-201 approved products list for PIV capability, as applicable to the use and purpose of the IoT device.
    b. Providing documentation describing how the IoT device can technically support PIV card implementation, accessibility and interfaces.
    c. Providing documentation with suggested ways in which customers can implement compensating controls around the IoT device if the IoT device cannot support PIV cards.
    d. Providing documentation explaining how to configure the IoT device to technically support PIV implementation, accessibility and interfaces.
    e. Providing detailed instructions for how to integrate the IoT device within a PIV system.
    f. Providing an attestation, from an authoritative source, that the IoT device can be used in compliance with Federal agency requirements, with associated descriptions for how the agency can accomplish this, if the IoT device cannot be integrated within a PIV system.
5. Establish communications detailing the IoT device interface and access controls capabilities. Information that may be necessary to provide include details and actions such as:
    a. Providing details for how to implement IoT device logical and remote access controls through device interfaces for data transmission between devices and subjects, objects, systems and components within the system.
    b. Providing documentation describing all the IoT device logical and remote interface access controls.
    c. Providing detailed instructions for how to restrict access to the IoT device interface for both users of the interface, and for the data that can be transmitted through that interface, and describing if and how interface restrictions can be defined.
    d. Providing copies of the manufacturer's policies and practices that govern how and with whom the manufacturer shares the data obtained from the manufacturer's IoT device.

[7] The FIPS-201 approved products list can be found at https://www.idmanagement.gov/approved-products-list-piv/

e. Providing the details and instructions to establish management and operational controls on and/or to the IoT device.
f. Providing details and descriptions about the specific types of manufacturer's needs to access the IoT device interfaces; such as for specific support, updates, ongoing maintenance, and other types of purposes.
g. Providing documentation describing the manufacturer requirements for collecting data from the IoT device, including the specific types of data being collected.
h. Providing documentation with instructions for the IoT device customer to follow for how to restrict interface connections that enable specific activities.
i. Providing descriptions of the types of access to the IoT device the manufacturer will require on an ongoing or regular basis.
j. Providing detailed instructions for how to implement management and operational controls based on the role of the IoT device user, and not on an individual basis.
k. Providing information and detailed instructions for how to establish, change and technically enforce role-based access settings and capabilities built within the IoT device, such as admin, general user, and other types of roles.
l. Providing information and instructions describing how role-based access settings and capabilities for the IoT device can be established, changed and technically enforced using hardware, software and/or firmware that is outside of the IoT device.

6. Establish communications describing situations where identification and authentication are not needed for the IoT device. Information that may be necessary to provide include details and actions such as:
    a. Providing detailed instructions and guidance for establishing activities performed by the IoT device that do not require identification or authentication.
    b. Providing a description of the privacy protection capabilities built within the IoT device that do not require authentication.
    c. Providing a description for how to access the IoT device through the logical access interface without authentication, as applicable to the purpose of the device.
7. Establish communications explaining how to provide monitoring information to authorized personnel or roles. Information that may be necessary to provide to support customer's needs to provide monitoring reports to specific roles within their organization include details and actions such as:
    a. Providing information that describes the types of system monitoring information generated from, or associated with, the IoT device and instructions for obtaining that information.

   b. Providing documentation describing the types of monitoring tools with which the IoT device is compatible, and recommendations for how to configure the IoT device to best work with such monitoring tools.
8. Establish communications describing how the IoT device cybersecurity event data is protected from unauthorized access, modification, and deletion. Information that may be necessary to provide include details and actions such as:
   a. Providing documentation and/or other communications describing how to implement management and operational controls to protect data, obtained from IoT devices, and associated systems and intrusion-monitoring tools, from unauthorized access, modification, and deletion.
   b. Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device.
9. Establish communications describing capabilities supporting IoT device data integrity, secure data handling and data retention. Information that may be necessary to provide include details and actions such as:
   a. Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.
   b. Providing detailed information listing capabilities that are required by data protection regulations.
   c. Providing detailed instructions for how to implement management and operational controls for securely handling and retaining IoT device data, associated systems data, and data output from the IoT device.
   d. Providing documentation describing how to irreversibly delete data from the IoT device.
   e. Providing detailed instructions for how to protect device data from being accidentally modified.
10. Establish documentation describing IoT device security requirements that can be used to support customers' organizational mission, business process planning, and IoT device acquisitions requirements. To support these needs, include details within documentation and associated actions such as:
   a. Providing detailed information describing the resources necessary for each type of security capability used with the IoT device.
   b. Providing instructions and/or information describing the recommended methods and tools for protecting the IoT device hardware, software and data, and the associated resources necessary to support them.
   c. Providing detailed instructions for how to establish restrictions for the acquisition of IoT devices, systems and services to only assigned organizationally-defined personnel or roles.

d. Providing documentation that clearly details the IoT device security and privacy capabilities and limitations, the specific types of manufacturer support that will be provided throughout the life of the device, supported operating systems compatible with the IoT device, and other information pertinent to the use and security of the device.

11. Establish documentation and communications describing the types of legal compliance the IoT device supports. Information that may be necessary to provide to support customer legal compliance needs, include details and actions such as:
    a. Providing documentation describing the legal (Federal regulations, state and local laws) requirements for security and privacy controls that the IoT device supports.
    b. Providing information describing how the manufacturer stays up-to-date with regulations, laws, and other legal requirements and standards that apply to IoT devices.
    c. Providing white papers and use cases of existing IoT device customers describing how they used the IoT device in ways that supported their legal compliance requirements needs.
12. Establish communications and documentation that detail the expected lifespan of the device, the expected time for supporting the device, the costs for maintaining the device, the costs for device parts replacements, costs for device repairs, and other costs related to using the IoT device. Information that may be necessary to provide include details and actions such as:
    a. Providing detailed information about the anticipated costs associated with the IoT device purchase, usage activities, repairs, maintenance, parts, operations, security, and disposal costs throughout the potential lifetime of the IoT device.
13. Establish communications that describes the manufacturer's third party, contractor, and vendor IoT device security oversight, and for including security and privacy requirements within contractual agreements. Information that may be necessary to provide to explain supply chain risk management include details and actions such as:
    a. Communications, detailed descriptions, methods, techniques, and/or policies the manufacturer uses to monitor IoT device activities and associated systems security control compliance by external service providers on an ongoing basis.
    b. Providing detailed information describing how the IoT device manufacturer performs oversight activities for their supporting entities, including such information as:
        - How the manufacturer meets legal and/or regulatory safeguard requirements related to supply chain risk management.
        - Details about the activities performed by each of the supporting entities to whom the manufacturer outsources IoT device support activities, and how such activities are monitored.

- The ways in which security and oversight requirements are included within contracts with entities throughout the supply chain for the IoT device.
- Remote monitoring activities the manufacturer performs for each of the supporting entities' activities.
- Description of the other access and data collection, use and sharing activities the supporting entities perform in support of the IoT devices, and how the manufacturer provides monitoring for these activities.

c. Communications and documentation detailing how the IoT device supports regulatory requirements for auditing and monitoring capabilities. Such information should list the external supporting entities throughout the supply chain that are involved with these activities, the specific activities and data that the supporting entities access while providing these activities, and the oversight that the manufacturer provides for the supporting entities.
d. Providing the detailed instructions for how IoT customers can implement and consistently use methods and techniques to monitor the IoT device and associated systems security control compliance of the manufacturer's supporting entities on an ongoing basis.
e. Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the manufacturer's supporting entity's monitoring service.
f. Communicating the manufacturer's procedure for how customers can provide feedback when the manufacturer's supply chain security management and logging practices do not meet established compliance requirements of IoT device customers' external service providers.

14. Establish communications detailing the security and privacy requirements the manufacturer includes within their supporting entity contractual agreements that cover access to, and/or use of, the IoT device by third parties. Information that may be necessary to provide include details and actions such as:
    a. Providing within the IoT device customer contracts a description and listing of the third parties used by the manufacturers that will have access to the IoT device and/or the data collected, generated, accessed, processed, or shared through the device, and a description of the associated security and privacy controls established for such third parties.
    b. Providing documentation detailing all the cloud services used to support the IoT device.
    c. Providing a detailed description of all logical interfaces to the IoT device and documenting the interfaces used by the manufacturer's third parties, and the purposes for such uses.

d. Providing the IoT device customers with a list of the third parties to whom the manufacturer provides the IoT device data and/or customer information.
e. Providing the IoT device customers with a list of the types of data provided to the third parties directly from and/or by the device (e.g., device usage, entities using the device, device location, personal data, etc.).
f. Providing the IoT device customers a detailed description of the other types of devices, systems, etc., that will be accessing the IoT device during customer use of the device, and how they will be accessing it.
g. Providing within the IoT device customer contracts, disclosures and/or similar types of documents, describing the actions the manufacturer will take for requested modification of interface capabilities, the supporting entities involved, and descriptions for how device customers should make such requests.
h. Providing a detailed description for how the IoT device customer will be notified of changes in the activities of the manufacturer's contractors and third-parties that have access to the IoT devices, such as when the origination or locations (e.g., city, state, country) of the contractors or third parties change, and other related types of contractor and third-party changes.
i. Providing a detailed description of the methods by which the manufacturer prevents unauthorized access to the customer's IoT device by third-parties not listed on the provided documentation.
j. Providing a detailed description for how third-parties are, or can be, prohibited by the IoT device customers from accessing the IoT device and/or restricted in their access to the device.
k. Providing a detailed description for the ways in which the manufacturer and/or the manufacturer's listed supporting entities, will be accessing and making modifications to the IoT device throughout the expected or typical lifespan of the IoT device.
l. Providing a description to Federal agencies for how the IoT device supports the Federal Risk and Authorization Management Program (FedRAMP) requirements.

(CAP) Technical Cybersecurity Capabilities Implemented

Description: Document the technical cybersecurity capabilities, such as those detailed within NISTIR 8259A and within the full IoT cybersecurity technical catalog, that are implemented within the IoT device and how to configure and use them.

Discussion: Non-technical communications and actions to explain how to most effectively use the technical abilities of an IoT device will help customers understand how to configure and implement the technical IoT device cybersecurity capabilities to limit the risks the IoT device brings to their systems. It will also help IoT device customers to comply with their

associated legal requirements and support their organizational purchasing requirements.

Related SP 800-53 Rev. 5 Controls: CM-6, CA-7, IA-4, MA-3, SA-5, SA-8, SI-4, SI-5, SI-7

Requirements that may be necessary:

1. Establish communications detailing the ways in which the IoT device capabilities connect to and communicate with diagnostic tools used by the manufacturer and/or supporting entities to support customers' legal requirements. Information and documentation that may be necessary to provide about the IoT device technical capabilities include details and actions such as:
    a. Providing the details necessary for IoT device customers to implement only organizationally-approved IoT device diagnostic tools within their system.
    b. Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.
2. Establish communications explaining how to use monitoring systems, possible monitoring activities, the use of devices and tools, and descriptions of security level changes. Information that may be necessary to provide include details and actions such as:
    a. Providing the details necessary for IoT device customers to monitor IoT devices and associated systems.
    b. Providing documentation to IoT device customers describing how to perform monitoring activities.
    c. Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.
    d. Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems.
    e. Providing documentation to the IoT device customers that describes indicators of unauthorized use of the IoT device.
    f. Providing documentation to IoT device customers describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems.
    g. Providing documentation to IoT device customers describing how and when to heighten the level of security for an IoT device and associated systems.
    h. Providing documentation to IoT device customers describing how to use the security controls and monitoring capabilities built within the IoT device, and how to configure the device to best fit the risk levels within the systems where they are used.
    i. Providing the details necessary to implement management and operational controls for when and how to generate internal security alerts, advisories, and directives about the IoT devices.

3. Establish communications to provide the IoT device customers with the details necessary to establish and modify IoT device data integrity controls. Information that may be necessary to provide include details and actions such as:
    a. Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.
    b. Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity.
4. Establish communications describing how to establish unique identification for the IoT device. Information that may be necessary to provide, as determined by the manufacturer's assessment of cybersecurity risk created by the IoT device, include details and actions such as:
    a. Providing details for how to establish unique identification for each IoT device associated with the system and critical system components within which it is used.

(DSC) Design and Support Considerations

Description: Document device design and support considerations related to the IoT device.

Discussion: Documentation describing the design of the device and associated cybersecurity capabilities, such as how IoT platforms were used in the development of the device, as well as documentation of the supporting entities involved with support activities throughout the manufacturer's supply chain may be important to meet the organization's purchasing requirements, to support audits, or to qualify for specific certifications that some customers may require for IoT devices they use.

Related SP 800-53 Rev. 5 Controls: AC-2, AC-6, IA-2, IA-3, SA-3, SA-5, SA-8, SR-3, SR-3(2), SR-3(3), SR-4, SR-8(32)

Requirements that may be necessary:

1. Establish communications with detailed instructions for using authentication techniques supported by IoT platforms. Information that may be necessary to provide include details and actions such as:
    a. Providing documentation describing the specific IoT platforms used with the device to support required IoT authentication control techniques.
    b. Providing documentation with details about the capabilities of the IoT platform used to support device interface controls, and descriptions for if and how a second factor for authentication can be implemented.

   c. Providing documentation with details describing external authentication IoT platforms, and associated authentication methods, that can be used with the IoT device.
2. Establish communications that provide details about the security capabilities of the IoT device software components. Information that may be necessary to provide describing the technical security capabilities include details and actions such as:
   a. Providing details about how the security capabilities of the IoT device software components meet regulatory and other legal and policy requirements.[8]
3. Establish communications for the IoT device customers with details for the security capabilities of the hardware components. Information that may be necessary to provide describing the security capabilities of hardware components include details and actions such as:
   a. Providing the IoT device customers with details about the security capabilities of the IoT device hardware components.
4. Establish communications providing IoT device management details that can be incorporated within the IoT device customer's system development life cycle. Information that may be necessary to provide about IoT device security management include details and actions such as:
   a. Providing the details necessary for customers to 1) manage the IoT device within their system using their organizationally-defined system development life cycle's associated information security considerations, 2) assign individuals with IoT device information security roles and responsibilities, and 3) integrate the IoT device within the organizational information security risk management process.
   b. Providing communications and the detailed instructions for implementing a hierarchy of privilege levels to use with the IoT device and/or necessary associated information systems.
   c. Providing communications with instructions and recommendations for how to incorporate IoT device management and associated security management, within the system development life cycle.
5. Establish communications that provide details about the manufacturer's supply chain risk management process and the controls used within ongoing supply chain security assessment and authorization activities. Information that may be necessary to provide about supply chain risk management include details and actions such as:
   a. Providing documentation explaining how the manufacturer provides security oversight of their supporting entities, and how they assess the cybersecurity

[8] This information may be provided by a Software Bill of Materials (SBOM).

risks that those supporting entities present to the IoT devices and the systems within which they are implemented.

b. Providing documentation and information describing the security requirements included within the contractual requirements for the supporting entities. Such requirements may include implementing security practices, safeguards, access controls and assessments to provide oversight of the supporting entities' activities.
c. Providing documentation describing the types of security and/or privacy certifications the manufacturer requires of their supporting entities.
d. Providing documentation of the manufacturer's Secure Software Development practices [SSDF] and methods to ensure that suppliers and other supporting entities also use secure development practices.
e. Providing documentation of controls employed to limit harm from potential adversaries identifying and targeting the manufacturer or manufacturer's supply chain and other supporting entities.

(MNT) Maintenance Requirements

Description: Document maintenance requirements for the IoT device.

Discussion: Documentation about maintenance requirements, especially involving supporting entities the manufacturer contracted to perform maintenance, device changes, etc., supports the customer's need to adequately plan for maintenance activities. Such documentation may also be necessary to meet the organization's purchasing requirements, security policies, to support audits, or to qualify for specific certifications that some customers may require for IoT devices they use.

Related SP 800-53 Rev. 5 Controls: AC-2, MA-1, MA-2, MA-4, MA-5, RA-5, SA-5, SI-1, SI-4, SI-12(3)

Requirements that may be necessary:

1. Establish communications describing the specifications and providing instructions for performing IoT device maintenance and repairs, for IoT device systems review, and for maintenance activities following trigger events. Information that may be necessary to provide for device maintenance and repairs include details and actions such as:
    a. Providing the details and instructions necessary to perform necessary IoT device maintenance activities and repairs.
    b. Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.

c. Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform. If such comprehensive IoT device maintenance operations documentation does not exist, the manufacturer should clearly communicate to IoT device customers that the user must perform these operations themselves.
d. Providing the details necessary for IoT device customers to perform required IoT device systems reviews.
e. Providing documentation that includes the suggested frequency of system review and maintenance activities for the IoT device.
f. Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.
g. Providing communications and documentation detailing how to perform account management activities, using the technical IoT device capabilities, or through supporting systems and/or tools.
h. Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.
i. Providing communications and documentation detailing the manufacturer's recommended vulnerability and patch management plan.

2. Establish communications with instructions for removing all data from IoT devices prior to maintenance and repairs. Information that may be necessary to provide include details and actions such as:
    a. Providing IoT device customers the details necessary for them to know when and how to remove all data from IoT devices prior to removing the devices from facilities for offsite maintenance or repairs.
    b. Providing information describing how to use the IoT device capabilities to remove all data from the device.
3. Establish communications to provide the IoT device customers with the details necessary to support IoT device maintenance and diagnostic activities and documentation. Information that may be necessary to provide include details and actions such as:
    a. Providing the details necessary to enable IoT device customers to monitor onsite and offsite IoT device maintenance activities.
    b. Providing the details necessary for maintaining records for nonlocal IoT device maintenance and diagnostic activities.
    c. Providing the details necessary to implement management and operational controls for IoT device maintenance personnel and associated authorizations, and record-keeping of maintenance organizations and personnel.
    d. Providing communications describing the type and nature of the local and/or remote maintenance activities that will involve and require manufacturer

personnel, or their contractors, once the device is purchased and deployed in the IoT device customer's organization.

e. Providing IoT device customers with the details necessary to implement management and operational controls in support of their security policies and legal requirements for IoT device maintenance for assigned organizationally-defined personnel or roles to follow.
f. Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.

(DAU) Device Authenticity Support

Description: Document information and/or processes that attest to and can help verify the authenticity of the IoT device and its internal components.

Discussion: Organizations may employ system-wide component authenticity controls, which may need to be supported by the IoT device. Anti-counterfeiting and authenticity measures may also need to be employed for the hardware and software within the IoT device. Sources of counterfeit hardware and software include, but are not limited to manufacturers, developers, vendors, and contractors.

Related SP 800-53 Rev. 5 Controls: SR-11

IQ - INFORMATION AND QUERY RECEPTION

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

Discussion: This capability provides an input for the manufacturer to use to gather cybersecurity related information about their IoT devices as they are being used by customers, revealing topics where there may be a need to provide additional customer training, along with tracking information provided to customers to answer their questions about securing the device. Such ongoing interactions have an important role in securing the IoT device and meeting customers' cybersecurity needs and goals after purchase. These actions can also support a number of other cybersecurity supporting activities, including those within the Information Dissemination and Education and Awareness non-technical supporting sections of capabilities. Organizations may also need to have such capabilities to meet organizational requirements related to conditions for making technology purchases, to support updates to management about how discovered problems or flaws within the IoT device are being addressed, and to maintain a history of documentation for specific IoT devices that could be considered when situations arise where other types of IoT devices are proposed to replace the existing IoT device. Organizations and their third-parties may want, or be required by contract, law and/or policy, to report vulnerabilities to manufacturers that they identify in an IoT device, or the systems that interface with or are incompatible with the device. Some customers may need additional support from the manufacturer to securely provision and use an IoT device.

Sub-Capabilities that may be necessary:

(BUG) Reception of Vulnerability Information

Description: The ability for the manufacturer and/or supporting entity to receive maintenance and vulnerability information from their customers and other types of entities.

Discussion: Organizations may want, or be required, to report vulnerabilities they identify within or related to an IoT device. These communications and actions also allow customers to ask questions related to the security of the IoT device, as well as provide input for the manufacturer to then use in the Information Dissemination and Education and Awareness non-technical supporting capability.

Related SP 800-53 Rev. 5 Controls: SI-2

Requirements that may be necessary:

1. Establish methods for the customer to report software flaws to the manufacturer with the details necessary for the manufacturer to fix the software flaws. Information that may be necessary to provide to support efficient software flaw reporting include details and actions such as:

a. Providing the details necessary to identify the type of software flaw, describe the characteristics of the flaw, and provide any suggestions for the manufacturer to consider when determining how to fix the software flaw.
b. Providing instructions for the IoT device customer to use to send the manufacturer software flaw reports.
c. Providing a description of the procedures the manufacturer follows for processing the software flaw reports, determining which flaws need to be fixed, for scheduling corrections to identified flaws, and for how the manufacturer will notify the IoT customer of the status of the software flaw fix.
d. Communicating device remediation efforts with stakeholders and IoT device customers.
e. Providing instructions for the IoT device customer to use to send other types of IoT device bug reports to the manufacturer.

(QRY) Query Response

Description: The ability for the manufacturer and/or supporting entity to respond to customer and third-party queries about cybersecurity of the IoT device (e.g., customer support).

Discussion: Manufacturers and/or their supporting entities can use methods such as providing trained personnel to respond directly to queries. Manufacturers can use reports of common queries and vulnerabilities to identify ways to improve the cybersecurity of the IoT device.

Related SP 800-53 Rev. 5 Controls: IA-1, MA-6, PM-20, PM-26, SA-4, SI-5

Requirements that may be necessary:

1. Establish communications with the details necessary for answering customer questions about implementing cybersecurity event awareness and control directives. Information that may be necessary to provide include details and actions such as:
    a. Providing customers with answers that include the details necessary to implement IoT device and associated systems security directives for cybersecurity events in accordance with established time frames.
    b. Providing customers with a method of contacting the manufacturer to obtain answers to questions about cybersecurity events related to the IoT device, and related cybersecurity requirements noncompliance.
2. Establish ways for IoT device customers to document attempts to obtain the IoT device components or information. Information that may be necessary to provide include details and actions such as:

   a. Providing the details necessary for IoT device customers to document attempts to obtain IoT device components, or IoT device information system service documentation when such documentation is either unavailable or nonexistent, and documenting the appropriate response for manufacturer employees, or supporting entities, to follow.
   b. Following procedures to obtain input from IoT device customers about the breadth and depth of the technical documentation provided with the IoT device to determine if it is acceptable to support customer needs.
3. Establish customer communications methods to the manufacturer to allow for questions about the security of the IoT device, ask for help with securing the IoT device, or related questions. Information and actions that may be necessary to provide to IoT device customers include:
   a. Providing a process to IoT device customers to follow to contact the manufacturer to ask questions or obtain help related to the minimum requirements they need to implement for the IoT device configuration settings.
4. Establish a customer services support communications capability to respond to customer calls and queries. Information that may be necessary to provide to IoT customers, as well as the manufacturer's' internal or external supporting call center staff, include details and actions such as:
   a. Providing the details necessary for IoT device customers to contact the manufacturer's call center with questions, concerns, or to report potential security or privacy problems with their IoT device.
   b. Establishing policies and procedures for call center staff to follow to verify the identity of customers.
   c. Establishing policies and procedures for call center staff to follow to document IoT device customer calls.
   d. Providing an online communications portal for IoT device customers to use to receive and respond to security questions, report areas of concern, and other IoT device related communications.

ID - INFORMATION DISSEMINATION

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

Discussion: Organizations will want to stay informed about the cybersecurity of IoT devices to allow them to fine tune their mitigations and maintain an adequate level of risk assurance. Organizations may need to know the security practices of the manufacturer and/or supporting entities that have made or will have occasional or ongoing access to the IoT devices to enable them to ensure the other parties do not unacceptably add to the customer's cybersecurity risk. Organizations may also want to view security certifications, accreditations and evaluations for what is typically third-party assurance of acceptable information describing cyber, networking, applications, and related security practices. Customer organizations can use the associated documentation to support their evaluation of the adequacy of the security provided by the manufacturer and/or supporting entities and related IoT device, including whether they comply with the associated laws and regulations for which they are covered can use the documentation to support their IoT purchase decisions and risk assessments.

Sub-Capabilities that may be necessary:

(CRI) Cybersecurity Related Information Alert

Description: The procedures to support the ability for the manufacturer and/or supporting entity to alert customers about cybersecurity relevant information.

Discussion: This sub-capability supports on-going cybersecurity of the device by keeping customers informed of developments and new information after the initial documentation was developed and provided. Organizations may need to be informed about cybersecurity-related activities on the IoT device, especially if the IoT device is critical to their operations. Manufacturers and/or their supporting entities can provide security alerts, advisories and other types of information to maintain situational awareness throughout the IoT device customer's system.

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

Requirements that may be necessary:

1. Establish communications with the details necessary for maintaining IoT device data integrity during software modifications. Information that may be necessary to provide about maintaining data integrity during software modifications include details and actions such as:
    a. Providing details for how to review and update the IoT device and associated systems while preserving data integrity.
    b. Providing information detailing the trigger events that will result in automated updates to the IoT devices, or will indicate the need for a manual update.

c. Providing communications with details about updates and possible impacts to IoT device data integrity (e.g., alerting users if an update will delete data).

2. Establish communications with the details necessary to meet customer requirements for software updates for flaw remediation and security-relevant reasons. Information that may be necessary to provide include details and actions such as:
    a. Providing details for performing the tests necessary for IoT device and related system software updates related to flaw remediation, for effectiveness and to identify potential side effects before installation.
    b. Providing communications describing the types of security and privacy tests necessary for the IoT device and software before installation.
    c. Providing the details necessary for the installation of IoT devices and associated systems security-relevant software updates within an organizationally-defined time period from the vendor release of the updates.
3. Establish communications describing the security impacts of using the IoT device when the manufacturer no longer supports or provides functionality for the IoT device. Information that may be necessary to provide include details and actions such as:
    a. Providing information with the details necessary to determine exceptions and/or alternatives to replacing unsupported IoT devices.
    b. Providing information to allow for in-house support from within the IoT device customer organization.
    c. Providing information with the details describing service contract completion and the situations that define the end of the system integrator or external service provider relationship. This is important to know for re-compete, potential changes in providers, and also to manage system end-of-device-life processes.
4. Establish communications with the details for responding to privacy and security and maintenance alerts, advisories, and directives from outside of their organization. Information that may be necessary to provide include details and actions such as:
    a. Providing information with the details necessary to disseminate privacy and security alerts, advisories, and directives about the IoT devices, and associated systems and then take the necessary actions.
    b. Providing information to IoT device customers necessary to inform the review and update of the IoT device systems and services practices.
5. Establish communications with information necessary for IoT device customers to receive the manufacturer's external and internal security alerts, advisories, and directives. Information that may be necessary to support alerts, advisories and directives include details and actions such as:
    a. Providing information with the details necessary to implement management and operational controls for how and when IoT device customers will receive

up-to-date security and privacy information from the manufacturer or supporting entity.

b. Providing information with the details and instructions necessary to receive the manufacturer's security and privacy updates, such as IoT device information system security and privacy alerts, advisories, directives, security and/or privacy research, and other information that would be valuable for IoT device customers to help ensure security and privacy of the IoT device.
c. Providing information to IoT device customers to inform them when to review and update the IoT device systems, based upon specific device states, and to provide a description of the services practices.

6. Establish communications notifying IoT device customers they should review and update the IoT device, systems and services acquisition practices. Information that may be necessary to provide for such updates and services include details and actions such as:
    a. Providing the instructions for following the manufacturer's updates to the IoT device, systems and services acquisition practices.
    b. Providing the details necessary for IoT device customers to document attempts to obtain IoT device components, or IoT device system service information when such information is either unavailable or nonexistent, and documenting the appropriate response for the manufacturer's employees to follow.
7. Establish communications with the details necessary for performing periodic IoT device security checks and/or audits. Information that may be necessary to provide about performing security checks and audits include details and actions such as:
    a. Providing the details requested by IoT device customers to perform periodic checks and/or audits to ensure IoT device security controls are functioning as intended following maintenance and repairs.
    b. Providing IoT device customers, upon their request, with the tools, assistance, instructions, and other support for the IoT device to perform audit and log maintenance and repairs operations.

(VNT) Cybersecurity Event Notification

Description: The procedures to support the ability for the manufacturer and/or supporting entity to notify customers of cybersecurity related events and information related to an IoT device throughout the support lifecycle.

Discussion: A well-defined manufacturer cybersecurity support life cycle provides the foundation for the successful and secure implementation and operation of IoT devices within customer systems. Organizations will want to stay informed about the cybersecurity of IoT devices throughout the lifetime of the device to allow them to fine tune their mitigations and maintain an adequate level of risk assurance.

Related SP 800-53 Rev. 5 Controls: IR-6, SR-8

Requirements that may be necessary:

1. Establish communications to notify customers of cybersecurity related events throughout the full time that the IoT device is in use. Information that may be necessary to provide include details and actions such as:
    a. Providing communications for cybersecurity related events involving or related to the IoT device.
2. Establish communications for responding to IoT device breaches, associated fixes to vulnerabilities allowing the breaches, and breaches that have occurred for similar types of IoT devices. Information that may be necessary to provide include details and actions such as:
    a. Providing security incident and breach information in a timely manner.
    b. Using notification and communications that include incident and breach information for the customer's IoT device.

EA - EDUCATION AND AWARENESS

Description: The ability for the manufacturer and/or supporting entity to create awareness of, and educate IoT device customers about, cybersecurity-related information, considerations, features, and other information related to reducing the risks created by the IoT device being implemented within the IoT customer's digital ecosystem.

Discussion: This capability supports secure provisioning and on-going cybersecurity support for using the IoT device. For IoT devices with a wide range of use cases, some customers may need more education than others to securely provision and use the device. The complexities of IoT systems, devices, and use cases makes it important for manufacturers to create awareness and educate customers about cybersecurity risks, capabilities, and related issues for their IoT devices. Manufacturers and/or their supporting entities can provide education to IoT device customers covering a wide range of topics, and determine the content of IoT device customer security training and awareness based on such factors as the specific organizational requirements of IoT device customers, the purpose of and capabilities within the IoT device, and other topics as determined by the results of the manufacturer performing an IoT device risk assessment and taking into consideration the questions and concerns communicated to them from their customers, through the activities in the capability Manufacturer Information and Query Reception. Education may occur through many forms; in-person, videos, online modules, training booklets, or some other form. The education content should ultimately address the needs for IoT device customers to know how to use the IoT device securely and include such topics as those described in this capability set of actions.

Sub-Capabilities that may be necessary:

(CSC) Cybersecurity Capabilities

Description: Educate customers of the IoT device about the presence and use of device cybersecurity capabilities.

Discussion: The complexities of IoT systems, devices, and use cases means it is important for manufacturers to create awareness and educate customers about the cybersecurity capabilities of their IoT device to help ensure IoT device customers (and possibly users if distinct from the customer) understand how to use such technical capabilities. This information will help IoT device customers to determine the degree to which the manufacturer's non-technical support will help them use the technical IoT device cybersecurity capabilities to support their security and purchasing policies and associated legal requirements.

Related SP 800-53 Rev. 5 Controls: AC-2, AC-3, AT-1, AT-2, CM-1, CM-2, CM-5, CM-6, IA-4, MA-3(6), PM-26, SI-2

Requirements that may be necessary:

1. Provide education explaining how to establish and require unique identification for each IoT device. Information that may be necessary to provide within the education activities include details and actions such as:
    a. Providing IoT device customers with the details necessary to establish and implement unique identification for each IoT device associated with the system and critical system components within which it is used.
    b. Providing IoT device customers with the details necessary to require unique identifiers for each IoT device associated with the system and critical system components within which it is used.
2. Provide IoT device customers with the education necessary to establish the IoT device configuration settings and requirements. Education topics that may be necessary to provide include details and actions such as:
    a. Providing IoT device customers with the education necessary to teach them how to establish then implement the minimum required IoT device configuration settings.
    b. Providing IoT device customers with education demonstrating how to ensure the configuration changes can be performed only by authorized entities.
    c. Providing education detailing how to set the minimum configuration settings available within the IoT device, and how to change those settings, to meet customers' needs and requirements.
    d. Providing education explaining the process IoT device customers need to follow to contact the manufacturer to ask questions or obtain help related to the minimum requirements for the IoT device configuration settings.
3. Provide education for how to establish the IoT device access controls. Education that may be necessary to provide include details and actions covering topics such as:
    a. Providing education explaining how to establish and enforce approved authorizations for logical access to IoT device information and system resources.
    b. Providing education explaining how to control access to IoT devices implemented within IoT device customer information systems.
    c. Providing education explaining how to enforce authorized access at the system level.
4. Provide education explaining how to establish software update functionality. Education that may be necessary to provide include details and actions such as:
    a. Providing education explaining how to inspect IoT device and/or use maintenance tools to ensure the latest software updates and patches are installed.
    b. Providing education for how to scan for critical software updates and patches.

(EOL) End-of-Life (Reprovisioning and Disposal)

Description: Educate customers about how an IoT device can be securely reprovisioned or disposed of.

Discussion: IoT devices, associated data, documentation, tools, or system components can be disposed of at any time during the device life cycle (not only at the end of life or service). For example, disposal of an IoT device's components and/or data by an organization can occur during research and development, design, prototyping, or operations and maintenance and can be accomplished using a wide range of methods. Opportunities for compromise during disposal affect physical and logical data.

Related SP 800-53 Rev. 5 Controls: AT-3, MP-6, SI-12

Requirements that may be necessary:

1. Provide education explaining how to implement security safeguards within customers' IoT device data handling and retention practices. Education topics that may be necessary to provide include details and actions such as:
    a. Providing educations describing how to securely handle and retain IoT device data, associated systems data, and data output from the IoT device, to meet requirements of the IoT device customers' organizational security policies, contractual requirements, applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and other legal requirements.
    b. Providing education that explains and/or demonstrates how to securely and irreversibly to delete data from the IoT device and any associated data storage locations.

(RSP) Cybersecurity Responsibilities

Description: Make customers aware of their cybersecurity responsibilities related to the IoT device and how responsibilities may be shared between them and others, such as the IoT device manufacturer.

Discussion: Manufacturers and/or their supporting entities can provide basic and advanced levels of IoT device security training, using the best training method as it relates to the customers of the devices, the type of IoT devices, and other related factors, describing the customer's responsibilities for IoT device security activities, such as those related to maintenance of the IoT device. This sub-capability can help organizations fulfill their responsibilities related to the operation of the IoT device within the context of their own systems within which the IoT device is implemented, and in accordance with their own security and privacy programs.

Related SP 800-53 Rev. 5 Controls: AC-3(7), AC-5, AT-1, AT-3, MA-1

Requirements that may be necessary:

1. Provide education explaining in detail how to perform IoT device maintenance. Education that may be necessary to provide include covering details and actions such as:
    a. Providing education that explains the legal requirements governing IoT device maintenance responsibilities, or how to meet specific types of legal requirements when using the IoT device.
    b. Providing education and supporting materials to ensure the individuals filling the established IoT device customer roles understand the requirements for specified maintenance procedures.
    c. Providing education and supporting materials to support the responsibilities for IoT device customer's data security roles.
    d. Providing education and supporting materials to IoT device customers explaining how to establish roles and responsibilities for IoT device data security, using the device capabilities and/or other services that communicate or interface with the device.
    e. Providing education and supporting materials describing the IoT device capabilities for role-based controls, and how to establish different roles within the IoT device.
    f. Providing education and supporting materials for how to establish roles to support IoT device policies, procedures and associated documentation.
    g. Providing education and supporting materials to be used by IoT device customer personnel with information security responsibilities, and others as determined appropriate.
    h. Providing education and supporting materials explaining recommended IoT device roles and responsibilities to support the ability for IoT device customers to determine the appropriate level within their organizational hierarchy of privileges to establish those roles.

(EXP) Cybersecurity Expectations and Assumptions

Description: Provide training to IoT customers that explains the manufacturer's key assumptions and expectations related to the cybersecurity of the IoT device.

Discussion: Manufacturers and/or their supporting entities can provide education and associated supporting materials describing the key assumptions for how the IoT device will be used, the needed types of physical, administrative and systems security controls that are expected to be implemented to support the strongest security for the IoT device, and the expectations the manufacturer has related to the use of the IoT device.. This sub-capability can help organizations be aware of the manufacturer and supporting entities' expectations and assumptions for how the IoT device will be used.

Related SP 800-53 Rev. 5 Controls: AT-3, RA-3

Requirements that may be necessary:

1. Provide education that clearly describes the assumptions and expectations for how the IoT device customers will manage risk for the IoT device. Information that may be necessary to provide include details and actions such as:
    a. Providing education explaining the responsibilities of IoT device customers to perform their own risk assessments using the information provided by the manufacturer, to determine the risks the IoT device will bring into the IoT device customer's systems.

(BAK) Data Back-up

Description: Provide training for how to back-up the data collected from or derived by the IoT device, and how to access such data that is stored in cloud storage, or other repositories.

Discussion: Data backups must be made to support IoT device customers' organizational requirements and as required by each organization's applicable laws, executive orders, directives, regulations, or other legal requirements regarding specific categories of information (e.g., personal health information). Manufacturers can provide education explaining and/or demonstrating how to back-up the data collected, derived from, stored, transmitted and/or processed by the IoT device, in addition to the IoT device system-level information including, if applicable, system state information, operating system software, middleware, application software, and licenses.

Related SP 800-53 Rev. 5 Controls: CP-9

Requirements that may be necessary:

1. Provide training explaining how to create and restore from IoT device data backups. Education and supporting materials that may be necessary to provide include details and actions such as:
    a. Providing education to IoT device customers covering the instructions and details necessary for them to create accurate backups, and to recover the backups when necessary.
    b. Providing education to IoT device customers that includes instructions describing how to back up data from systems where IoT device data is stored.
    c. Providing awareness reminders and tips to IoT device customers (e.g., directly in person, in videos, in an online webinar) for various aspects involved with backing up the IoT device data.

(VMG) Vulnerability Management Options

Description: Educate customers about threat and vulnerability management options available for the IoT device or associated system that could be used by customers.

Discussion: Manufacturers and/or their supporting entities can provide education describing the IoT device and/or manufacturer's threat and vulnerability monitoring for IoT device components, ensuring that potential threats are not overlooked. Education about vulnerability management options will provide organizations with the knowledge necessary for them to most effectively manage risk within the systems where the IoT device is implemented.

Related SP 800-53 Rev. 5 Controls: CM-3, CM-4, IR-8, IR-4, RA-3, SI-2, SI-3

Requirements that may be necessary:

1. Provide education that describes the details necessary for malicious code protection, detection and eradication. Information that may be necessary to provide, as determined by the manufacturer's assessment of cybersecurity risk created by the IoT device, include details and actions such as:
    a. Providing education to IoT device customers for how to implement malicious code protection in the IoT device and associated systems, as well as within related systems entry and exit points, and how to detect and eradicate malicious code.
    b. Providing education to IoT device customers for how to update the IoT device and related systems malicious code protection mechanisms when new releases are available, in accordance with organizational configuration management policy and procedures.
    c. Providing training and awareness information to IoT device customers that describe newly identified vulnerabilities and threats (such as zero-day malware) for the associated IoT device.
    d. If the IoT device manufacturer provides anti-malware for the associated IoT device, or if the IoT device has built-in anti-malware capabilities, the manufacturer should provide education to the IoT device customers describing how to use and/or configure malicious code protection mechanisms in IoT devices, supporting anti-malware tools, and related systems.
    e. Providing education describing the operational impacts of the anti-malware activities on mission critical processes in the system where the IoT device is used.
    f. Providing education describing the options and recommended responses to malicious code identification within the IoT device.

g. Providing education that include the details necessary to implement management and operational controls for malicious code detection and eradication.

2. Provide education explaining and/or showing how to incorporate IoT device flaw remediation into the customer's configuration management process. Education and supporting materials that may be necessary to provide include details and actions such as:
    a. Providing the education explaining how to incorporate IoT device flaw remediation into the IoT device customer's organizationally-defined configuration management process.
    b. Providing the education explaining the processes that the manufacturer, or supporting entities, will follow to communicate the IoT device remediation efforts with stakeholders (IoT device customers, users, etc.).

References

[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

[800-53] 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

[800-63] Grassi P, Garcia M, Fenton J (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Includes updates as of March 2, 2020. https://doi.org/10.6028/NIST.SP.800-63-3

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

[CMVP] National Institute of Standards and Technology (2021) Cryptographic Module Validation Program. Available at https://nist.gov/cmvp

[FIPS-140] National Institute of Standards and Technology (2002) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3

[FIPS-180] National Institute of Standards and Technology (2015) Secure Hash Standard (SHS). (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 180-4. https://doi.org/10.6028/NIST.FIPS.180-4

[FIPS-201] National Institute of Standards and Technology (2013) Personal Identity Verification (PIV) of Federal Employees and Contractors. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 201-2. https://doi.org/10.6028/NIST.FIPS.201-2

[FIPS-202] National Institute of Standards and Technology (2015) SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 202. https://doi.org/10.6028/NIST.FIPS.202

[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

[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

[NIST FIPS] National Institute of Standards and Technology (2021) [Federal Information Processing Standards]. Available at https://csrc.nist.gov/publications/fips

[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—Definition of the Federal Profile for IoT Device Cybersecurity Requirements

The following profile (referred to as the federal profile) of the IoT device cybersecurity capability core baseline [8259A] and non-technical supporting capability core baseline [8259B] was created using the security guidance provided to federal government organizations and non-federal users (i.e., NIST SP 800-53 Rev. 5 [800-53]). The federal profile elaborates on the core baseline and non-technical baseline using the controls from the low-impact RMF baseline from SP 800-53B [800-53B] as guidance. Device cybersecurity capabilities and non-technical supporting capabilities were selected from the catalog for inclusion in the federal profile based on those that would support the low impact baseline. The federal profile is a useful starting point to identify device cybersecurity requirements (i.e., device cybersecurity capabilities and non-technical supporting capabilities). In some cases, the capabilities in the federal profile may be sufficient for an organization to support their selected and tailored security controls and achieve their security capabilities, but this profile may not reflect the IoT device cybersecurity requirements for specific organizations. For example, the assumptions made in creating the federal profile and resulting device cybersecurity capabilities and non-technical supporting capabilities may not be sufficient to meet a specific organization's needs. Additionally, specific organizations may tailor controls and/or use common or compensating controls that may render some capabilities in the profile not applicable or insufficient to meet the specific organization's needs. Finally, other organization goals beyond cybersecurity (e.g., safety, privacy, reliability, resilience) that may be just as critical to the organization's mission may further impact device cybersecurity requirements in ways the federal profile cannot capture. For these reasons, the federal profile must be considered in the context of the guidance provided in SP 800-213 [800-213].

The federal profile is presented in two tables. Table 1 details the device cybersecurity capability abilities in the federal profile. Table 2 details the non-technical supporting capability actions in the federal profile. Each row in each table represents one sub-capability¬, which is a collection of abilities or actions that redefine, expand, and/or specify the core capabilities from the IoT core baseline using additional context from the sector and/or use case. These are grouped into seven core IoT technical capabilities that manufacturers may have to design and build into IoT devices: Device Identity, Device Configuration, Data Protection, Logical Access to Interfaces, Software Update, Cybersecurity State Awareness, and Device Security. A group of sub-capabilities are all related to their associated core capability but may or may not relate to each other. Similarly, abilities or actions within a sub-capability all relate to the sub-capability but not necessarily to each other. The arrangement of abilities or actions into sub-capabilities in the federal profile is not meant to represent a formal definition of sub-capabilities, and other users of this profile or creators of other profiles may arrange abilities and actions into sub-capabilities that are most meaningful for their organization, sector, and/or use case. For the federal profile, sub-capabilities are grouped such that they reflect support for a specific control or approach to enable easier tailoring of this profile for specific organizations. Sub-capabilities are described by:

- First column: the sub-capabilities and corresponding requirements across presented in this catalog that are part of the federal profile. Where a subset of a sub-capability's list of

"*requirements that may be necessary*" applied to the federal profile, those specific requirements are identified. Otherwise, the inclusion of all the "*requirements that may be necessary*" or lack of specific requirements to select from is noted.

- Second column: the primary SP 800-53 Rev. 5 controls possibly supported (based upon use case) by the sub-capability. This sub-capability is necessary based upon the context for how the IoT device is used and the associated risk, but may not be sufficient by itself to implement the control for a device. For example, there may need to be a capability for the device to have an identifier to implement the control AU-3 Content of Audit Records to support audit system logging of information about the device.

Table 1 below defines the device cybersecurity capabilities (i.e., technical capabilities implemented within the device) in the federal profile. The capabilities from the IoT device cybersecurity capability core baseline are used to arrange the sub-capabilities in the profile.

Table 1: Device Cybersecurity Capabilities from Catalog Identified for Federal Profile

Sub-Capability (requirements)	Possible SP 800-53 Rev. 5 Controls Supported
Device Identity (DI)	
Identifier Management Support (IMS) (1) (3)	IA-3, **IA-4**
Actions Based on Device Identity (AID) (2) (3) (4)	IA-3, **AC-3**, **SI-4, AU-2, CM-8**
Device Configuration (DC)	
Logical Access Privilege Configuration (PRV) (*sub-capability does not list specific requirements*)	**AC-3, CM-5**
Authentication and Authorization Configuration (AUT) (*sub-capability does not list specific requirements*)	**AC-3, CM-5**
Interface Configuration (INT) (*sub-capability does not list specific requirements*)	**AC-3**, **CM-5**
Display Configuration (DSP) (*sub-capability does not list specific requirements*)	**AC-8,** AC-12(2), AC-12(3)
Device Configuration Control (CTL) (*all requirements*)	**CM-2,** CM-3, **CM-5**, **CM-6, SR-11(2)**
Data Protection (DP)	
Cryptography Capabilities and Support (CRY) (*all requirements*)	**SC-13**, SC-17
Cryptographic Key Management (KEY) (*all requirements*)	**SC-12,** SC-12(6), **SC-13,** SA-9(6)
Secure Storage (STO) (*all requirements*)	SC-28, **MP-6,** CP-9(8)
Logical Access to Interfaces (LA)	
Authentication Support (AUN) (*all requirements*)	**IA-2, IA-2(1), IA-2(2), IA-6,** AC-17(10)
Authentication Configuration (ACF) (1) (3)	AC-2(2), AC-2(3), AC-2(5), AC-3(8), **AC-7,** AC-9, **AC-17**, IA-8
System Use Notification Support (USE) (*all requirements*)	**AC-8**
Authorization Support (AUZ) (*all requirements*)	**IA-2**
Authentication & Identity Management (AIM) (*sub-capability does not list specific requirements*)	**AC-14**
Role Support & Management (ROL)	**AC-2**, **AC-3**, AC-6, AC-21, IA-4, SC-2

(1) (2) (3) (6) (7) (9)	
Interface Control (IFC) (*all requirements*)	**AC-2**, **AC-3,** AC-6, AC-21, IA-4, SC-2
Software Update (SU)	
Update Capabilities (UPD) (*all requirements*)	**AU-1,** CM-3, **CM-5,** CM-14, SI-7(15)
Update Application Support (APP) (*all requirements*)	**SI-2**
Cybersecurity State Awareness (CS)	
Access to Event Information (AEI) (*all requirements*)	**SI-4, AU-11, AU-12**
Event Identification & Monitoring (EIM) (*all requirements*)	**AU-2,** AU-13, **CA-7,** CM-3, **CM-6, IA-2**, **SC-7**, **SC-15**, SC-42, **SI-4**
Event Response (EVR) (*all requirements*)	**AU-6,** CP-13, **SC-15**, SC-42, **SI-4, RA-7**
Logging Capture & Trigger Support (LCT) (*all requirements*)	**AU-2**, **AU-3**
Support of Required Data Logging (RDL) (*all requirements*)	**AU-2**, **AU-3**, **AU-4**, AU-5(1), AU-5(5), **AU-11**
Audit Log Storage & Retention (LSR) (all requirements)	**AU-4,** AU-5(1), **AU-11**
Support for Reliable Time (SRT) (2) (3) (4)	**AU-8,** SC-45(1)
Audit Support & Protection (AUP) (1) (2) (3) (4) (6)	AU-5(5), **AU-6,** AU-7, AU-9, **SI-4**
Device Security (DS)	
Secure Execution (EXE) (*all requirements*)	SC-2, **SC-39**
Secure Communication (COM) (*all requirements*)	SC-7, SC-7(17), SC-10, SC-11, **SC-21,** SC-23, SC-16(2), SC-51, SI-14(3), SI-10(6)
Secure Resource Usage (RSC) (*all requirements*)	CP-12, SC-4, **SC-5**, SC-24, SC-34, **SC-39**, SI-17
Secure Device Operation (OPS) (*all requirements*)	CM-2(7), **CM-7**, **CP-10**, CP-12, IR-4(5), PE-10, **PE-12, PE-13, PE-14, PE-15,** SC-24, SC-45, SC-45(1), SI-6

Table 2 below defines the non-technical supporting capabilities in the federal profile. These are arranged by four core IoT non-technical supporting capabilities that manufacturers or third parties may have to provide related to IoT devices: Documentation, Information and Query reception, Information Dissemination, and Education and Awareness. Sub-capabilities are arranged using the IoT device non-technical supporting capability core baseline.

Table 2: Non-Technical Supporting Capabilities from this Catalog Identified for Federal Profile

Sub-Capability (requirement)	Primary SP 800-53 Rev. 5 Controls Supported
Documentation (DO)	
Assumptions made in Product Development (SMP) (1) (2) (3) (5) (6) (7) (8) (9) (10) (11) (12) (13) (14)	**MA-1**, MA-3, **PE-3, PE-6, PL-1**, **IA-1**, **IA-2**, **IA-4, SI-1, SI-4, SI-5,** SI-7, **SI-12**, SI-21, **SA-2, SA-4, SA-8, SR-3, SR-5, AC-1, AC-3,** AC-3(7), **AC-14**, PT-4, PT-5, **PS-6**, **AT-3**, PM-20, **CA-7**, **CM-6**
Technical Cybersecurity Capabilities Implemented (CAP) (*all requirements*)	**SI-4**, **CA-7, SA-8, CM-6**, **SI-5**, **IA-4**, MA-3, SI-7
Design and Support Considerations (DSC) (*all requirements*)	**IA-2**, **AC-2**, **SA-3, SR-3,** SR-3(2), SR-3(3), SR-4, **SR-8, SA-8,** AC-6
Maintenance Requirements (MNT)	**MA-1**, **MA-2, MA-4, MA-5, SI-1**, **SI-4, AC-2**, **RA-5, SI-12**

(*all requirements*)	
Device Authenticity Support (DAU) (*sub-capability does not list specific requirements*)	**SR-11**
Information and Query Reception (IQ)	
Reception of Vulnerability Information (BUG) (*all requirements*)	**SI-2**
Query Response (QRY) (1)	**SI-5, SA-4,** PM-20, PM-26, MA-6
Information Dissemination (ID)	
Cybersecurity Related Information Alert (CRI) (*all requirements*)	**SR-8**, **SI-2,** SA-10, **CM-4**, RA-9, **SA-22, SI-5, SA-4,** PM-26, **MA-1**
Cybersecurity Event Notification (VNT) (*all requirements*)	**SR-8, IR-6**
Education and Awareness (EA)	
Cybersecurity Capabilities (CSC) (*all requirements*)	**IA-4, CM-1, AT-1**, **AT-2**, **CM-5, AC-2**, **AC-3, CM-2**, **CM-6,** PM-26, MA-3, **SI-2**
End-of-Life (EOL) (*all requirements*)	**SI-12**, **MP-6**
Cybersecurity Responsibilities (RSP) (*all requirements*)	**MA-1**, **AT-1**, **AT-3**, **AC-3**, AC-5
Cybersecurity Expectations and Assumptions (EXP) (*all requirements*)	**RA-3, AT-3**
Data Back-up (BAK) (*all requirements*)	**CP-9**
Vulnerability Management Options (VMG) (*all requirements*)	**SI-2**, **SI-3, RA-3,** CM-3, **CM-4**, **IR-8**, **IR-4**

Appendix B—Mapping of SP 800-53 Controls to Device Cybersecurity Requirements

Mapping of device cybersecurity capabilities and non-technical supporting capabilities to SP 800-53 controls is included with each sub-capability in this catalog, but organizations may also find value in starting with SP 800-53 controls and mapping to device cybersecurity requirements. The table below lists SP 800-53 controls and the corresponding device cybersecurity or non-technical supporting capability that may be necessary to support the control.

RMF Control	NIST SP 800-213A Technical Capabilities	NIST SP 800-213A Non-Technical Capabilities
AC-1		DO: SMP(5e,f,g,h)
AC-2	LA: ROL(1), ROL(2), ROL(3), ROL(4), ROL(6)	DO: DSC(2a), MNT(1g) EA: CSC(3a,b,c)
AC-2(1)	LA: ROL(6)	
AC-2(2)	LA: ACF(1)	
AC-2(3)	LA: ACF(1), ACF(3)	
AC-2(5)	LA: ACF(1)	
AC-2(7)	LA: ROL(5), ROL(6)	
AC-2(8)	LA: ROL(7)	
AC-3	DI: AID(1) DC: PRV(1), AUT(1), INT(1) LA: ROL(1), ROL(3), ROL(9), IFC(4), IFC(5), IFC(7), IFC(9), IFC(15)	DO: SMP(8a) EA: CSC(2c), CSC(3a,b,c), RSP(1g)
AC-3(7)	LA: ROL(2), ROL(4)	DO: SMP(3b), SMP(5j) EA: RSP(1d,e,f)
AC-3(8)	LA: ACF(3)	
AC-4		
AC-5		EA: RSP(1h)
AC-6	LA:ROL(5),LA:IFC(4),LA:IFC(5)	DO: DSC(4b)
AC-7	LA:ACF(1)	
AC-8	DC: DSP(1) LA: USE(1), USE(2), USE(3)	
AC-9	LA: ACF(1)	
AC-10	LA: LDU(2), XCN(5)	
AC-11		
AC-12		
AC-12(2)	DC: DSP(1)	
AC-12(3)	DC: DSP(1)	
AC-14	LA: AIM(1)	DO: SMP(6a)
AC-16		
AC-17	LA: ACF(2), IFC(1)	
AC-17(4)	LA: IFC(8)	
AC-17(10)	LA: AUN(4)	
AC-18	LA: IFC(13), IFC(14), IFC(15)	
AC-19		
AC-20		
AC-21	LA: ROL(8), LDU(1), XCN(1), XCN(2), XCN(3)	
AC-22		
AC-23		
AC-24		
AC-25		
AT-1		EA: CSC(2a,b), RSP(1d,e,f)

RMF Control	NIST SP 800-213A Technical Capabilities	NIST SP 800-213A Non-Technical Capabilities
AT-2		EA: CSC(2a,b), CSC(3b,c)
AT-3		DO: SMP(5k,l), EOL(1a,b), RSP(1c,d,e,f,g), EXP(1a)
AT-4		
AT-6		
AU-1	SU: UPD(2)	DO: SMP(13c)
AU-2	DI: AID(2) CS: EIM(3), LCT(1), RDL(1), RDL(2), RDL(3), RDL(4), RDL(6), SRT(4)	
AU-3	CS: LCT(1), RDL(1), RDL(2), RDL(5)	
AU-4	CS: RDL(6),CS:LSR(1)	
AU-5	CS: EVR(7)	
AU-5(1)	CS: RDL(7), LSR(4)	
AU-5(5)	CS: RDL(7), AUP(5)	
AU-6	CS: EVR(3), EVR(4), AUP(1), AUP(2), AUP(4)	
AU-7	CS: AUP(3)	
AU-8	CS: SRT(1), SRT(3), SRT(4)	
AU-9	CS: AUP(1), AUP(2), AUP(4), AUP(6), AUP(7)	DO: SMP(8b)
AU-10		
AU-11	CS: AEI(2), RDL(3), LSR(2), LSR(3)	
AU-12	CS: AEI(2)	
AU-13	CS: EIM(5)	
AU-14		
AU-16		
CA-1		
CA-2		
CA-3		
CA-5		
CA-6		
CA-7	CS: EIM(1), EIM(2), EIM(4), EIM(5), EIM(6), EIM(7), EIM(8), EIM(9), EIM(10)	DO: CAP(2c,f)
CA-8		
CA-9		
CA-9(1)	DS: DIN(1)	
CM-1		EA: CSC(2a,b)
CM-2	DC: CTL(1), CTL(2)	EA: CSC(2d)
CM-2(3)	SU: UPD(3)	
CM-2(7)	DS: OPS(4)	
CM-3	DC: CTL(1) SU: UPD(2) CS: EIM(7)	EA: VMG(2a)
CM-4		EA: VMG(1e)
CM-4(1)		ID: CRI(2b)
CM-5	DC: PRV(1), AUT(1), INT(1), CTL(2), CTL(4), LA: IFC(10) SU: UPD(1), UPD(4), UPD(5)	EA: CSC(2c)
CM-6	DC: CTL(4) CS: EIM(7)	DO: CAP(2g,h) EA: CSC(2d)
CM-7	LA: IFC(2), IFC(3), IFC(6), IFC(13), IFC(15) DS: OPS(8)	
CM-8	DI: AID(3), AID(4)	
CM-8(3)	DS: DIN(2), DIN(4)	
CM-8(8)	DI: AID(4)	
CM-9		
CP-9(8)	DP: STO(3)	
CM-10		

RMF Control	NIST SP 800-213A Technical Capabilities	NIST SP 800-213A Non-Technical Capabilities
CM-11		
CM-12		
CM-13		
CM-14		
CP-1		
CP-2		
CP-3		
CP-4		
CP-6		
CP-7		
CP-8		
CP-9	DP: STO(3)	EA: BAK(1a,b,c)
CP-10	DS: OPS(3)	
CP-11		
CP-12	DS: RSC(6), OPS(3), OPS(4), OPS(6)	
CP-13	CS: EVR(10)	
IA-1		DO: SMP(4d,e,f) IQ: QRY(4b)
IA-2	LA: AUN(1), AUZ(1), AUZ(2) CS: EIM(4)	DO: DSC(1a, b, c)
IA-2(1)	LA: AUN(2)	DO: SMP(4b,c)
IA-2(2)	LA: AUN(2)	
IA-3	DI: IMS(1), IMS(2), AID(1), AID(4), DAS(1), DAS(2), PID(1)	DO: DSC(1a,c)
IA-3(1)	DS:ONB(1),DS:ONB(2)	
IA-4	DI: IMS(3), LA: ROL(1), ROL(3)	DO: CAP(4a) EA: CSC(1a,b)
IA-5	DS: ONB(2), ONB(3)	
IA-6	LA: AUN(3)	
IA-7		
IA-8	LA: ACF(2)	
IA-9		
IA-10		
IA-11		
IA-12		
IR-1		
IR-2		
IR-3		
IR-4	CS: EVR(2)	EA: VMG(1f)
IR-4(5)	DS: OPS(7)	
IR-5		
IR-6		ID: VNT(2a,b)
IR-7		
IR-8		EA: VMG(1f)
IR-9		
MA-1		DO: SMP(1f, g), MNT(3a) ID: CRI(7a,b) EA: RSP(1a,b)
MA-2		DO: MNT(1a,b,c, h)
MA-3		DO: CAP(1a,b)
MA-3(6)		EA: CSC(4a,b)
MA-4		DO: MNT(1h), MNT(3b)
MA-5		DO: MNT(3c,d,e,f)
MA-6		IQ: QRY(2b)
MA-7		

RMF Control	NIST SP 800-213A Technical Capabilities	NIST SP 800-213A Non-Technical Capabilities
MP-1		
MP-2		
MP-3		
MP-4		
MP-5		
MP-6	DP: STO(4)	EA: EOL(1b)
MP-7		
MP-8		
PE-1		
PE-2		
PE-3		DO: SMP(2a,b,c)
PE-4		
PE-5		
PE-6		DO: SMP(2a,b,c)
PE-8		
PE-9		
PE-10	DS: OPS(9)	
PE-11		
PE-12	DS: OPS(9)	
PE-13	DS: OPS(9)	
PE-14	DS: OPS(9)	
PE-15	DS: OPS(9)	
PE-16		
PE-17		
PE-18		
PE-19		
PE-20		
PE-21		
PE-22		
PE-23		
PL-1		DO: SMP(3a)
PL-2		
PL-4		
PL-7		
PL-8		
PL-9		
PL-10		
PL-11		
PM-1		
PM-2		
PM-3		DO: SMP(12a)
PM-4		
PM-5		
PM-6		
PM-7		
PM-8		
PM-9		
PM-10		
PM-11		
PM-12		
PM-13		
PM-14		
PM-15		
PM-16		

RMF Control	NIST SP 800-213A Technical Capabilities	NIST SP 800-213A Non-Technical Capabilities
PM-17		
PM-18		
PM-19		
PM-20		DO: SMP(6b) IQ: QRY(4d)
PM-21		
PM-22		
PM-23		
PM-24		
PM-25		
PM-26		IQ: QRY(1b), QRY(2a), QRY(3a), QRY(4a,c,d) ID: CRI(6b) EA: CSC(2e)
PM-27		
PM-28		
PM-29		
PM-30		
PM-31		
PM-32		
PS-1		
PS-2		
PS-3		
PS-4		
PS-5		
PS-6		DO: SMP(5i)
PS-7		
PS-8		
PS-9		
PT-1		
PT-2		
PT-3		
PT-4		
PT-4(1)		DO: SMP(5c)
PT-5		DO: SMP(5d), SMP(6c), SMP(14a,b,c,d,e,f,g,h,i,j,k,l)
PT-6		
PT-7		
PT-8		
RA-1		
RA-2		
RA-3		EA: EXP(1a), VMG(1c)
RA-5		DO: MNT(1i)
RA-6		
RA-7	CS: EVR(1), EVR(2), EVR(3), EVR(4), EVR(5), EVR(7), EVR(8), EVR(9), EVR(10), EVR(11)	
RA-8		
RA-9		ID: CRI(2c)
RA-10		
SA-1		DO: SMP(10c,d)
SA-2		DO: SMP(12a)
SA-3		DO: DSC(4a,c)
SA-4		IQ: QRY(2a) ID: CRI(6b)
SA-4(1)		DO: SMP(5a,b)
SA-4(2)		ID: CRI(6a)

RMF Control	NIST SP 800-213A Technical Capabilities	NIST SP 800-213A Non-Technical Capabilities
SA-4(10)		DO: SMP(4a)
SA-5		DO: SMP(1a,c,g), SMP(3a,b,c), SMP(4d,e), SMP(5a,b,c,e,h,j,k,l) , SMP(8a), SMP(9a,c), SMP(10d), CAP(1b), DO:CAP(2a,b,c,d,e,f,g,h,i), CAP(3a,b), CAP(4a), DSC(1a,b,1c), MNT(1a,b,c,d,e,f,g,h,i)
SA-8		DO: CAP(2g), CAP(2h)
SA-8(21)	CS: AWR(1)	
SA-8(32)		DO: SMP(1a,b,c,d,e), SMP(10a,b), DSC(3a)
SA-9		
SA-9(6)	DP: KEY(1)	
SA-10		
SA-10(1)		ID: CRI(1a)
SA-11		
SA-15		
SA-16		
SA-17		
SA-20		
SA-21		
SA-22		ID: CRI(3a,b,c)
SA-23		
SC-1		
SC-2	LA: ROL(4) DS: EXE(2), EXE(3)	
SC-3		
SC-4	DS: RSC(1)	
SC-5	DS: RSC(5), RSC(8)	
SC-6		
SC-7	CS: EIM(6) DS: COM(1), ONB(4)	
SC-7(17)	DS: COM(2)	
SC-8	DP: STX(2), STX(4) LA: XCN(1) DS: COM(7)	
SC-8(1)	DP: STX(1), STX(3)	
SC-10	DS: COM(3), COM(4), COM(5)	
SC-11	DS: COM(6)	
SC-12	DP: KEY(1)	
SC-16(2)	DS: COM(11)	
SC-12(6)	DP: KEY(1)	
SC-13	DP: CRY(1), CRY(2),CRY(3), CRY(4), CRY(5), KEY(1)	
SC-15	CS: EIM(8), EIM(9), EVR(5)	
SC-16	DS: ONB(1), ONB(3)	
SC-16(2)	DS: COM(11)	
SC-17	DP: CRY(2)	
SC-18		
SC-20		
SC-21	DS: COM(8)	
SC-22		
SC-23	DS: COM(7), COM(9), COM(10)	
SC-24	DS: RSC(6), OPS(3), OPS(5), OPS(6), OPS(8)	
SC-25		
SC-26		
SC-27		
SC-28	DP: STO(1), STO(2)	
SC-29		

RMF Control	NIST SP 800-213A Technical Capabilities	NIST SP 800-213A Non-Technical Capabilities
SC-30		
SC-31		
SC-32		
SC-34	DS: RSC(7), DIN(5)	
SC-35		
SC-36		
SC-37		
SC-38		
SC-39	DS: EXE(1), RSC(2), RSC(3), RSC(4)	
SC-40		
SC-41		
SC-42	CS: EIM(10), EVR(6)	
SC-43		
SC-44		
SC-45	DS: OPS(1), OPS(2)	
SC-45(1)	CS: SRT(2) DS: OPS(2)	
SC-46		
SC-47		
SC-48		
SC-49		
SC-50		
SC-51	DS: COM(3), RSC(9)	
SI-1		DO: SMP(9b), SMP(11a), MNT(1d)
SI-2	SU: APP(1), APP(2), APP(3)	IQ: BUG(1a,b,c,d,e) ID: CRI(2a) EA: CSC(4a,b), VMG(2a,b)
SI-3		EA: VMG(1a,b,d,g)
SI-4	DI: AID(2), CS: AEI(1), EIM(1), EIM(2), EIM(7), EIM(11), EIM(12), EVR(1), EVR(8), EVR(9), AUP(1), AUP(2)	DO: SMP(3c), SMP(7a,b), CAP(2a,b,d,e), MNT(1e,f)
SI-5		DO: CAP(2i) IQ: QRY(1a) ID: CRI(5a,b,c)
SI-5(1)		ID: CRI(4a,b)
SI-6	CS: AWR(1) DS: OPS(7)	
SI-7		DO: SMP(8a), SMP(9a), CAP(3a,b)
SI-7(15)	SU: UPD(6), UPD(7)	
SI-8		
SI-10		
SI-10(6)	DS: COM(12)	
SI-11		
SI-12		DO: SMP(9c) EA: EOL(1a)
SI-12(3)		DO: MNT(2a,b)
SI-13		
SI-14		
SI-14(3)	DS: COM(4)	
SI-15	LA: IFC(11), IFC(12)	
SI-16		
SI-17	DS: RSC(6)	
SI-18		
SI-19		
SI-20		

RMF Control	NIST SP 800-213A Technical Capabilities	NIST SP 800-213A Non-Technical Capabilities
SI-21		DO: SMP(9d,e)
SI-22		
SI-23		
SR-1		
SR-2		
SR-3		DO: SMP(13a,b,c,d,e,f), DSC(5a,b,c,d,e)
SR-3(2)		DO: DSC(5a,b,c,d,e)
SR-3(3)		DO: DSC(5a,b,c,d,e)
SR-4		DO: DSC(5a,b,d,e)
SR-5		DO: SMP(11b,c)
SR-6		
SR-7		
SR-8		DO: DSC(5a,b,c,d,e), CRI(1b,c), VNT(1a)
SR-9	DS: DIN(3)	
SR-9(1)	DS: DIN(3)	
SR-10		
SR-11		DO: DAU
SR-11(2)	DC: CTL(1), CTL(3)	
SR-12		

Appendix C—Mapping of Cybersecurity Framework Outcomes to Device Cybersecurity Requirements

Some organizations may use the Cybersecurity Framework (CSF) in addition to the RMF. To enable more efficient use of SP 800-213 for such organizations, the following mapping lists CSF outcomes and indicates which device cybersecurity capabilities and non-technical supporting capabilities could support the outcomes.

CSF	NIST SP 800-213A Technical Capabilities	NIST SP 800-213A Non-Technical Capabilities
IDENTIFY		
Asset Management		
ID.AM-1	DI: AID(4) DS: DIN(2)	DO: CAP(4a) EA: CSC(1a,b)
ID.AM-2	DI: AID(3)	
ID.AM-3		DO: SMP(14c,e)
ID.AM-4		DO: SMP(14b,c)
ID.AM-5		
ID.AM-6		
Business Environment		
ID.BE-1		
ID.BE-2		
ID.BE-3		
ID.BE-4		
ID.BE-5		
Governance		
ID.GV-1		
ID.GV-2		
ID.GV-3		DO: SMP(6b,c), SMP(9b), SMP(11a,b,c), SMP(13b,c), DSC(2a), MNT(1d,e), MNT(3a) IQ: QRY(1a,b) EA: EOL(1a), RSP(1a)
ID.GV-4		DO: SMP(12)(a)
Risk Assessment		
ID.RA-1		ID: CRI(2a,b) EA: VMG(1c)

CSF	NIST SP 800-213A Technical Capabilities	NIST SP 800-213A Non-Technical Capabilities
ID.RA-2		EA: VMG(1c)
ID.RA-3		
ID.RA-4		ID: CRI(2c) EA: VMG(1e)
ID.RA-5		EA: EXP(1a)
ID.RA-6		DI: CRI(2c)
Risk Management Strategy		
ID.RM-1	DS: DIN(1)	
ID.RM-2		
ID.RM-3		
Supply Chain Risk Management		
ID.SC-1		
ID.SC-2		DO: SMP(14d)
ID.SC-3		DO: SMP(1a,c,d,e,f,g), SMP(3a,b,c), SMP(4b,c,e,f), SMP(5a,b,c,d,e,f,g,h,i), SMP(7b), SMP(8b), SMP(9a), SMP(9b,d,e), SMP(10a,b,c,d), SMP(11b,c), SMP(12a), SMP(13a,b,c,d,e,f), SMP(14a,b,c,d,e,f,g,h,i,j,k,l), CAP(1a,b), CAP(2b,d,e,f), CAP(3a,b), DSC(1b), DSC(2a), DSC(3a), DSC(4a,b,c), DSC(5a,b,c,d,e), MNT(1b,c,d,e,f), MNT(2a,b), MNT(3a,c,d,e,f),DAU IQ: BUG(1a,b,c,d,e), QRY(1a,b), QRY(2a,b), QRY(3a) ID: CRI(1a,b,c), CRI(2a,b,c), CRI(3a,c), CRI(5a,b), CRI(6a,b), CRI(7a,b) EA: CSC(2)(a,c,d,e), EOL(1b), RSP(1a,b,h), VMG(1d)
ID.SC-4		DO: SMP(13a,d), DSC(5a,b,c,d,e)
ID.SC-5		
PROTECT		
Identity Management, Authentication & Access Control		
PR.AC-1	DI: IMS(1),IMS(2),IMS(3),AID(1),DAS(2),PID(1) LA: AUN(3), AUN(4), ACF(3), ROL(1), ROL(3), ROL(6)	DO: CAP(4)(a), MNT(1)(g) EA: CSC(1a,b), CSC(3a,b,c)

CSF	NIST SP 800-213A Technical Capabilities	NIST SP 800-213A Non-Technical Capabilities
	DS: ONB(3)	
PR.AC-2		DO: SMP(2a,b,c)
PR.AC-3	DI: AID(1) LA: ACF(2), XCN(1), XCN(4), XCN(5), IFC(1), IFC(7), IFC(8), IFC(9) CS: EIM(8), EIM(9), EIM(10)	
PR.AC-4	LA: ACF(3), AIM(1), ROL(2), ROL(4), ROL(5), ROL(6), ROL(7), ROL(8), ROL(9), LDU(1), LDU(2), IFC(4), IFC(5), IFC(7) DS: COM(9), COM(10), RSC(3), RSC(4), ONB(4)	DO: SMP(3b), SMP(5f,h,i,j), SMP(8a), SMP(14f), DSC(4b), MNT(1g) EA: CSC(3a,b,c), RSP(1d,e,f)
PR.AC-5		
PR.AC-6	DP: CRY(2) CS: EIM(4)	
PR.AC-7	DI: AID(1), DAS(1) LA: AUN(1), AUN(2), ACF(1), ACF(2), USE(1), USE(2), USE(3), AUZ(1), AUZ(2), ROL(6), ROL(9), XCN(5) DS: ONB(1), ONB(2)	DO: SMP(6a), DSC(1a,c)
Awareness and Training		
PR.AT-1		DO: SMP(4d) EA: CSC(1a,b), CSC(2a,b), CSC(3b,c), RSP(1b), RSP(1c), EXP(1a), BAK(1a,b,c), VMG(1a,b,c,d)
PR.AT-2		
PR.AT-3		EA: RSP(1c,d,e,f,h), EXP(1a)
PR.AT-4		
PR.AT-5		DO: SMP(5k,l)

CSF	NIST SP 800-213A Technical Capabilities	NIST SP 800-213A Non-Technical Capabilities
		EA: RSP(1g)
Data Security		
PR.DS-1	DP: CRY(1), CRY(2), CRY(5), KEY(1), STO(1), STO(2) CS: AUP(6)	DO: SMP(9c) EA: EOL(1a)
PR.DS-2	DP: CRY(1), CRY(5), KEY(1), STO(2), STX(1), STX(2), STX(3), STX(4) CS: AUP(6)	DO: SMP(8a) EA: EOL(1a)
PR.DS-3	DP: STO(4)	
PR.DS-4	DS: RSC(5), RSC(7), RSC(8)	
PR.DS-5	LA: IFC(11), IFC(12)	
PR.DS-6	DI: AID(3), CRY(3), CRY(4), CRY(5), STX(2), STX(3) SU: UPD(6), APP(1) CS: AUP(7) DS: COM(11), COM(12), RSC(9), DIN(3), DIN(5)	DO: SMP(8a), SMP(9a), CAP(3a,b) ID: CRI(1a)
PR.DS-7		
PR.DS-8	DS: DIN(3)	
Information Protection Processes and Procedures		
PR.IP-1	DC: PRV(1), AUT(1), INT(1), DSP(1), CTL(1), CTL(2), CTL(4) LA: IFC(2), IFC(6), IFC(15) SU: UPD(2) CS: RDL(3) DS: OPS(3), OPS(4)	DO: CAP(2g,h)
PR.IP-2	SU: UPD(1)	DO: CAP(2g), DSC(2a), DSC(3a), DSC(4a,c)

CSF	NIST SP 800-213A Technical Capabilities	NIST SP 800-213A Non-Technical Capabilities
	DS: DIN(3)	IQ: BUG(1a,b,c,d,e) ID: CRI(2a,b)
PR.IP-3	DC: PRV(1), AUT(1), INT(1), CTL(1), CTL(2), CTL(3), CTL(4) LA: IFC(9), IFC(10) SU: UPD(2), UPD(4), UPD(5), APP(1), APP(2), APP(3) CS: RDL(3)	ID: CRI(2a) EA: VMG(2a)
PR.IP-4	DP: STO(3)	EA: BAK(1a,b,c)
PR.IP-5	DS: OPS(9)	
PR.IP-6	DP: STO(4)	DO: SMP(9d), MNT(2a,b) EA: EOL(1b)
PR.IP-7		
PR.IP-8		
PR.IP-9		
PR.IP-10		
PR.IP-11		
PR.IP-12	SU: APP(3)	DO: MNT(1i)
Maintenance		
PR.MA-1		DO: SMP(1b,f,g), CAP(1a,b), MNT(1a,b,c,f,h), MNT(3a,c,d,e,f) IQ: QRY(2a), QRY(2b), QRY(3a) ID: CRI(3b), CRI(6b) EA: CSC(4a,b), RSP(1a)
PR.MA-2		DO: SMP(1b,f,g), MNT(1a,b,h), MNT(3b,c,d,e,f)
Protective Technology		

CSF	NIST SP 800-213A Technical Capabilities	NIST SP 800-213A Non-Technical Capabilities
PR.PT-1	CS: AEI(2), EIM(3), LCT(1), RDL(1), RDL(2), RDL(4), RDL(5), RDL(6), LSR(1), LSR(2), LSR(3), LSR(4), SRT(1), SRT(2), SRT(3), SRT(4), AUP(3), AUP(4), AUP(7) DS: EXE(1), OPS(1)	DO: SMP(9c) ID: CRI(7a,b)
PR.PT-2	DS: DIN(4)	
PR.PT-3	LA: IFC(2), IFC(3), IFC(6) DS: EXE(1), EXE(2), EXE(3), OPS(8)	
PR.PT-4	LA: IFC(13), IFC(14), IFC(15) DS: COM(1), COM(2), COM(3), COM(4), COM(5), COM(6), COM(7), COM(8)	
PR.PT-5	SU: UPD(3), UPD(7), CS: EVR(7), EVR(10), RDL(7), AUP(5), AWR(1) DS: RSC(6), OPS(3), OPS(4), OPS(5), OPS(6)	
DETECT		
Anomalies and Events		
DE.AE-1		DO: CAP(2f)
DE.AE-2	CS: EIM(1)	DO: CAP(2c)
DE.AE-3	CS: EVR(6), RDL(2)	DO: SMP(8b)
DE.AE-4		
DE.AE-5	CS: EVR(1), AWR(1)	
Security Continuous Monitoring		
DE.CM-1	DI: AID(2) LA: ACF(1) CS: AEI(1), EIM(2), EIM(5), EIM(6)	DO: SMP(7a,b), CAP(2a,b)

CSF	NIST SP 800-213A Technical Capabilities	NIST SP 800-213A Non-Technical Capabilities
DE.CM-2		DO: SMP(2a,b, c)
DE.CM-3		
DE.CM-4		EA: VMG(1a,b,d,g)
DE.CM-5		
DE.CM-6		DO: SMP(13a,c,d)
DE.CM-7	CS: EIM(5), EIM(7), EIM(8), EIM(9), EIM(10), EIM(11), EIM(12), EVR(8), EVR(9), DIN(4)	DO: SMP(13e), CAP(2a,d,e)
DE.CM-8		
Detection Processes		
DE.DP-1		
DE.DP-2	CS: AUP(2)	DO: DAU
DE.DP-3		
DE.DP-4	CS: EVR(3), EVR(4), EVR(5), AUP(1), AUP(4)	
DE.DP-5		
RESPOND		
Response Planning		
RS.RP-1	CS: EVR(2), EVR(7), EVR(11)	EA: VMG(1f)
Communications		
RS.CO-1		
RS.CO-2		ID: VNT(2a,b)
RS.CO-3	LA: ROL(8), XCN(2), XCN(3)	EA: VMG(2b)
RS.CO-4		EA: VMG(2b)
RS.CO-5		DO: SMP(9e), CAP(2i), MNT(1c) ID: CRI(4a,b), CRI(5c), VNT(1a) EA: VMG(2b)
Analysis		
RS.AN-1		
RS.AN-2		

CSF	NIST SP 800-213A Technical Capabilities	NIST SP 800-213A Non-Technical Capabilities
RS.AN-3	CS: AUP(3)	
RS.AN-4		
RS.AN-5		DO: CAP(2i) ID: CRI(1c), CRI(4a,b), CRI(5a,b,c), VNT(1a) EA: VMG(1c)
Mitigation		
RS.MI-1		
RS.MI-2		
RS.MI-3		EA: CSC(4a,b), VMG(2a)
Improvements		
RS.IM-1	CS: EVR(11) DS: OPS(7)	
RS.IM-2		
RECOVER		
Recovery Planning		
RC.RP-1		
Improvements		
RC.IM-1		
RC.IM-2		
Communications		
RM.CO-1		
RM.CO-2		
RM.CO-3		

Appendix D—Acronyms

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

EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
ITL	Information Technical Laboratory
NIST	National Institute of Standards and Technology
NISTIR	NIST Internal or Interagency Report
OMB	Office of Management and Budget
PEAP	Protected EAP
PIV	Personal Identity Verification
RMF	Risk Management Framework
SP	Special Publication
TCP	Transmission Control Protocol
TLS	Transport Layer Security
USB	Universal Serial Bus

Appendix E—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.