

# **Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government**

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

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.IR.8259D-draft>

# Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government

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

Rebecca Herold  
*The Privacy Professor  
Des Moines, IA*

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.IR.8259D-draft>

December 2020



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

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

National Institute of Standards and Technology Interagency or Internal Report 8259D  
30 pages (December 2020)

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.IR.8259D-draft>

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

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

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

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

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

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

## Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

### Abstract

The NISTIR 8259 series provide general guidance on how manufacturers can understand and approach their role in supporting customers' cybersecurity needs and goals. As discussed in those documents, specific sectors and use cases may require more specific guidance than what is included in the device capability core baseline in NISTIR 8259A and the non-technical and supporting capability baseline in NISTIR 8259B for IoT devices. This publication provides the profile created for the Federal Government using the process described in NISTIR 8259C, which can serve as a helpful starting point in determining and anticipating federal agencies' IoT device cybersecurity requirements.

### Keywords

Cybersecurity baseline; Internet of Things (IoT); securable computing devices; security requirements; Risk Management 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 Cybersecurity for IoT team members Brad Hoehn and David Lemire and the NIST FISMA Implementation Project team for their extensive help.

### Audience

The main audience for this publication is IoT device manufacturers. This publication may also help IoT device customers or integrators, particularly those that work in or with the federal government.

## Note to Reviewers

NIST Cybersecurity for IoT Team has chosen a publication strategy of crafting separate documents to address specific concerns within the IoT cybersecurity ecosystem. These documents are part of a single family across the theme of providing guidance to IoT device manufacturers. Industry encouraged this direction in the comments responding to the issuance of Draft NISTIR 8259. The initial foundation documents in this series are as follows:

- [NISTIR 8259](#): *Foundational Cybersecurity Activities for IoT Device Manufacturers*
- [NISTIR 8259A](#): *IoT Device Cybersecurity Capability Core Baseline*

The new documents in the series that are being released as drafts for comment provide guidance to IoT device manufacturers complementing the guidance in the initial foundational documents. The three additional documents in the NISTIR 8259 series are:

- ***NISTIR 8259B: IoT Non-technical and Supporting Capability Core Baseline*** – NISTIR 8259B complements the NISTIR 8259A device cybersecurity core baseline by detailing what additional, non-technical support is typically needed from manufacturers. This non-technical baseline collects and makes explicit support capabilities like documentation, training support, etc.
- ***NISTIR 8259C: Creating a Profile of the IoT Core Baseline and Non-Technical Baseline*** – NISTIR 8259C presents a method of profiling the baselines in NISTIR 8259A and NISTIR 8259B to create a more detailed set of capabilities responding to the concerns of a specific sector, based on some authoritative source such as a standard or other guidance. This is the method used to create the profile meeting the requirements of the federal information system low baseline.
- ***NISTIR 8259D: Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government*** – NISTIR 8259D presents the profile defining the capabilities needed from and related to IoT devices to incorporate those devices into a federal information system implementing the low baseline controls of NIST SP 800-53.

In addition to the extensions to NISTIR 8259 listed above, the NIST Cybersecurity for IoT Team is also working on **NIST SP 800-213: IOT Device Cybersecurity Guidance for the Federal Government: An Approach for Establishing IoT Device Cybersecurity Requirements** which explains from a customer organization's (i.e., federal agencies and other organizations) perspective how to determine the technical and non-technical capabilities needed from and related to devices to support the NIST SP 800-53 controls they use on their system and in their organization. NIST SP 800-213 enables federal agencies to identify needed capabilities for unique situations and turn those selections into requirements for new IoT devices.

NIST appreciates all comments, concerns and identification of areas needing clarification. Ongoing discussion with the stakeholder community is welcome as we work to improve the cybersecurity of IoT devices. **Community input is specifically sought regarding the mapping of specific reference document content to the items in Tables 1 and 2, to populate the fourth column, "IoT Reference Examples," to strongly align the NISTIR 8259D profile to the existing body of cybersecurity guidance. Table 1 in NISTIR 8259A can be used as a model for these informative reference mappings.**

153

## Call for Patent Claims

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

160

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

163

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

166

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

170

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

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

175

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

181

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

184

185 Such statements should be addressed to: [iotsecurity@nist.gov](mailto:iotsecurity@nist.gov)

186

**Table of Contents**

<b>1</b>	<b>Introduction .....</b>	<b>1</b>
<b>2</b>	<b>The Profile of the IoT Core Baseline and Non-Technical Baseline for the Federal Government .....</b>	<b>4</b>
<b>3</b>	<b>Conclusion .....</b>	<b>17</b>
	<b>References .....</b>	<b>18</b>

**List of Appendices**

<b>Appendix A— Acronyms .....</b>	<b>20</b>
<b>Appendix B— Glossary .....</b>	<b>21</b>

**List of Figures**

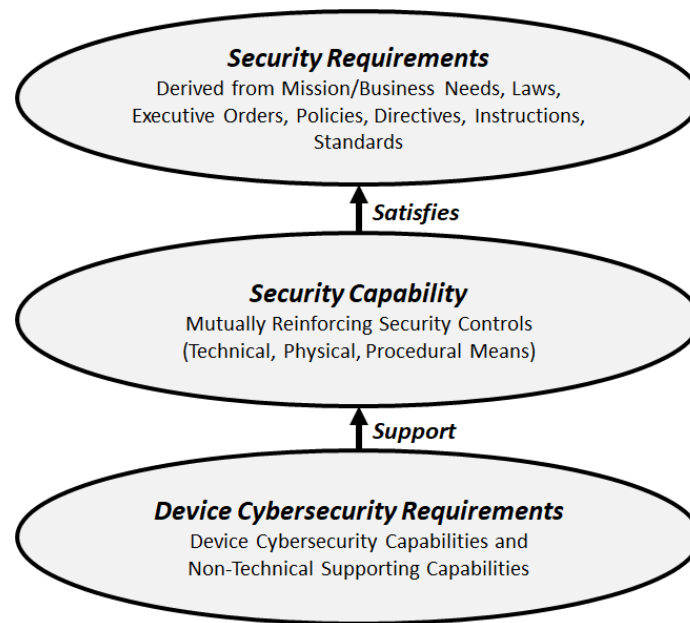
<b>Figure 1 - The Role of Device Cybersecurity Requirements in Supporting Customer Cybersecurity Requirements .....</b>	<b>1</b>
---	----------

**List of Tables**

<b>Table 1 - Device Cybersecurity Capabilities in the Federal Profile .....</b>	<b>5</b>
<b>Table 2 - Non-technical Supporting Capabilities in the Federal Profile .....</b>	<b>10</b>

## 1 Introduction

Many organizations<sup>1</sup> within the federal government are looking to acquire IoT devices. In many cases, these IoT devices will act as elements of larger systems<sup>2</sup>. As such, the ability for an organization to support the security<sup>3</sup> requirements of the associated system as well as those of the organization is often dependent on the capabilities offered by the IoT device and/or the manufacturer or affiliated third parties. IoT devices support these system and organizational security requirements by providing both technical (device cybersecurity) capabilities and non-technical (administrative and physical actions) supporting capabilities. As shown in Figure 1, these IoT device cybersecurity capabilities and non-technical supporting capabilities enable federal agencies to produce cybersecurity capabilities in their systems and organizations.



**Figure 1 - The Role of Device Cybersecurity Requirements in Supporting Customer Cybersecurity Requirements**

While cybersecurity is a shared responsibility, NISTIR 8259 *Foundational Cybersecurity Activities for IoT Device Manufacturers* [1] explains how manufacturers play a key role in building cybersecurity capabilities into IoT devices throughout the product development

<sup>1</sup> Similarly to how the term is defined in the Risk Management Framework, *organization* is meant to describe entities of any size, complexity, or positioning within an organizational structure.

<sup>2</sup> In some contexts, the larger system could be the organization's internal network which provides internal equipment connectivity and external Internet access. An example could be connecting an IoT camera to the existing federal information system. A *federal information system* is an information system used or operated by an agency, a contractor of an agency, or another organization on behalf of an agency.

<sup>3</sup> The terms *security* and *cybersecurity* are synonymous, but consistently used within this publication. Since the Risk Management Framework (RMF) uses the term *security*, when referring to specific concepts from that suite of publications, that term is used. In all other instances, the term *cybersecurity* is used, as is the convention in NISTIR 8259 and 8259A.



lifecycle starting at conceptualization through manufacturing and distribution<sup>4</sup>. Federal organizations may need the IoT devices they intend to purchase to provide particular device cybersecurity capabilities (e.g., access control or audit logging capabilities). Non-technical supporting capabilities (e.g., documentation or risk assessments) provided by the manufacturer or other third parties may also be needed to support the initial and on-going cybersecurity functionality of the IoT device.

For some organizations there may be a set of device cybersecurity and non-technical supporting capabilities considered to be required for an IoT device. Without these capabilities, organizations must compensate for risks that the device may introduce to the system and/or risks that the device cannot help the system mitigate. This set can be considered device cybersecurity requirements, which are distinct from the higher-level (e.g. organizational level) security requirements as shown in Figure 1. For more information about the federal agency perspective and how they may identify device cybersecurity requirements, see Draft NIST SP 800-213, *Guidance for Establishing Cybersecurity Requirements for IoT Devices to be used by the Federal Government* [2].

By designing IoT devices with cybersecurity device capabilities and providing non-technical supporting capabilities, manufacturers support organizations in meeting their cybersecurity requirements. Many organizations might have similar IoT device cybersecurity requirements to support system and organizational security capabilities. However, the IoT device cybersecurity requirements may vary among organizations for many reasons. Organizations can have variability in how they achieve system and organizational security capabilities (i.e., mutually reinforcing security controls) within their organization based on the intended purpose of the IoT device in consideration of the context within which it is used.<sup>5</sup> Additionally, the specific cybersecurity capabilities established via controls or how elements are expected to support those controls may vary across organizations, since organizations may employ tailoring or use compensating controls. Therefore, the specific device cybersecurity and non-technical supporting capabilities needed to provide/support security capabilities, as shown in Figure 1, may vary between organizations, even if the higher-level security capabilities, and security requirements are the same.

This publication is best understood within the context provided by NISTIR 8259, NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline* [3], NISTIR 8259B, *IoT Non-Technical Supporting Capability Core Baseline* [4], and NISTIR 8259C, *Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline* [5]. The 8259 series aims to help manufacturers understand how they play a role in their customers' cybersecurity. The IoT device

---

<sup>4</sup> Though this publication does not discuss lifecycle considerations specifically, they are considered by the authors and should not be ignored by manufacturers and/or customers when consider cybersecurity of IoT devices or any equipment. For more information about lifecycle considerations, please see NISTIR 7289, *The Role of Standards in Product Lifecycle Management Support* [6].

<sup>5</sup> For example, common controls (i.e., those provided to other elements through the system) may also be present and change the device cybersecurity requirements for an element, even if the security goal the common control achieves exists.

cybersecurity core baseline and non-technical supporting capability baseline<sup>6</sup> provide a starting point for manufacturers. NISTIR 8259C provides the guidance to create a profile of the needs and goals of specific customer sectors or use cases using that starting point. This publication will extend the NISTIR 8259 series by providing the profile of the core baseline and non-technical baseline for the federal government as a customer.

The determination of device cybersecurity capabilities and non-technical supporting capabilities for IoT draws on the long and well-established field of cybersecurity in general. Leveraging the wealth of existing cybersecurity guidance in the context of an IoT device's role in cybersecurity is particularly important when considering how an IoT device must support broader system and organizational cybersecurity needs and goals. This is highlighted throughout the NISTIR 8259 series. A single IoT device may not always be able to mitigate, on its own, all the risks it faces<sup>7</sup> or creates<sup>8</sup> and may need to provide cybersecurity capabilities that can be used to help the system and owner organization mitigate risks beyond those of the device itself and those the device creates. These are important considerations for any device that will be part of a bigger system, but the increasing scale and heterogeneity of IoT devices brings these issues to the forefront as enterprises, including federal agencies, look to use this new technology.

---

<sup>6</sup> As is the case across the entire NISTIR 8259 series, the usage of the term "baseline" in this publication should not be confused with the low-, moderate-, and high-impact system control baselines set forth in SP 800-53, *Security and Privacy Controls for Information Systems and Organizations* [7].

<sup>7</sup> For example, an IoT device used to remotely monitor a room within a home may risk being accessible by others remotely if it does not have sufficient cybersecurity capabilities implemented, such as to prevent unauthorized individuals from seeing into the room.

<sup>8</sup> For example, a smart fish tank that is implemented within the organization's system may provide a pathway into the system because of unimplemented and/or unsupported security controls.

## 2 The Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government

The following profile<sup>9</sup> (referred to as the federal profile) of the IoT device cybersecurity capability core baseline and non-technical supporting capability core baseline was created using the security guidance provided to federal government organizations and non-federal users (i.e., NIST SP 800-53 Rev. 5 and the Cybersecurity Framework [10]). The first step was to elaborate on the core baseline and non-technical baseline with a catalog<sup>10</sup> of device-centric, cybersecurity-focused capabilities that may be needed by federal government organizations to implement cybersecurity capabilities. Using the controls from the low-impact RMF baseline from SP 800-53B as guidance, device cybersecurity capabilities and non-technical supporting capabilities were selected from the catalog for inclusion in the federal profile. The low impact baseline provides a useful guide of minimal securability for the federal government and a starting point for the federal profile. The core baseline, non-technical baseline, and other well-documented concerns were also useful in defining the federal profile.

The federal profile is a useful starting point to identify device cybersecurity requirements (i.e., device cybersecurity capabilities and non-technical supporting capabilities) that would be expected from or related to an IoT device for many organizations that plan to integrate the device with their information systems. Though the federal profile may be used by organizations to supplement federal cybersecurity and privacy risk management guidance in NIST SP 800-37 *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [9] by identifying potential capabilities relevant for federal IoT devices, it will not supersede or replace the SP 800-37 and supporting risk management guidance for those organizations. Therefore, this profile may not reflect the IoT device cybersecurity requirements for specific organizations.

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

<sup>9</sup> For clarification of the specific use of the term profile, see definition of “profile” or “federal profile” in the glossary.

<sup>10</sup> The full catalogs from which the federal profile is derived, called the IoT Element Cybersecurity Requirement Catalogs can be found online at [pages.nist.gov](https://pages.nist.gov) [8].

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 name of the sub-capability. Related sub-capabilities commonly have similar or standard names. **Please Note:** sub-capabilities are numbered for reference purposes, and the assignment of numerals is not reflective of an explicit or implied ordering of sub-capabilities.
- Second column: the key abilities/actions of the sub-capability—aspects of the sub-capability that are key to defining the sub-capability and supporting cybersecurity needs and goals. For device cybersecurity capabilities, these are called *abilities*, referring to the abilities of the device, while for non-technical supporting capabilities, these are called *actions*, referring to actions taken by the manufacturer or third party.
- Third 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.
- Fourth columns: reference examples to external guidance that provide more information about the sub-capability. **Please Note:** this column is blank for the Public Comment draft as NIST looks to the public for recommended informative references for the proposed federal profile.

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 in the Federal Profile**

Sub-Capability	Key Abilities	Possible SP 800-53 Rev. 5 Controls Supported	Informative References
<b>Device Identity</b>			
1. Identifier Management Support	<ul style="list-style-type: none"> <li>• Ability for the device to support a unique device ID (e.g., to allow it to be linked to the person or process assigned to use the IoT device)</li> </ul>	<ul style="list-style-type: none"> <li>• IA-4, Identifier Management</li> </ul>	
2. Actions Based on Device Identity	<ul style="list-style-type: none"> <li>• Ability to monitor specific actions based on the IoT device identity</li> <li>• Ability to identify software loaded on the IoT device based on IoT device identity</li> </ul>	<ul style="list-style-type: none"> <li>• AU-3, Content of Audit Records</li> <li>• CM-8, System Component Inventory</li> </ul>	
3. Physical Identifiers	<ul style="list-style-type: none"> <li>• Ability to add a unique physical identifier at an external or internal location on the device authorized entities can access</li> </ul>	<ul style="list-style-type: none"> <li>• MP-4 Media Storage</li> <li>• PE-22 Component Marking</li> </ul>	
<b>Device Configuration</b>			

Sub-Capability	Key Abilities	Possible SP 800-53 Rev. 5 Controls Supported	Informative References
1. Display Configuration	<ul style="list-style-type: none"> <li>• Ability to configure content to be displayed on a device</li> </ul>	<ul style="list-style-type: none"> <li>• AC-8, System Use Notification</li> </ul>	
2. Device Configuration Control	<ul style="list-style-type: none"> <li>• Ability to change the device's software configuration settings</li> <li>• Ability for authorized entities to restore the device to a secure configuration defined by an authorized entity</li> <li>• Configuration settings for use with the Device Configuration capability including, but not limited to: <ul style="list-style-type: none"> <li>○ Ability for authorized entities to configure the cryptography use itself, such as choosing a key length</li> <li>○ Ability to configure any remote update mechanisms to be either automatically or manually initiated for update downloads and installations</li> <li>○ Ability to enable or disable notification when an update is available and specify who or what is to be notified</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• CM-2, Baseline Configuration</li> <li>• CM-3, Configuration Change Control</li> <li>• CM-6, Configuration Settings</li> </ul>	
<b>Data Protection</b>			
1. Cryptographic Capabilities & Support	<ul style="list-style-type: none"> <li>• Ability to execute cryptographic mechanisms of appropriate strength and performance</li> <li>• Ability to verify digital signatures</li> <li>• Ability to run hashing algorithms</li> <li>• Ability to compute and compare hashes</li> </ul>	<ul style="list-style-type: none"> <li>• SC-13, Cryptographic Protection</li> </ul>	
2. Cryptographic Key Management	<ul style="list-style-type: none"> <li>• Ability to change keys securely</li> <li>• Ability to generate key pairs</li> <li>• Ability to store encryption keys securely</li> </ul>	<ul style="list-style-type: none"> <li>• SC-12, Cryptographic Key Establishment and Management</li> </ul>	
3. Secure Storage	<ul style="list-style-type: none"> <li>• Ability to "sanitize" or "purge" specific or all data in the device</li> </ul>	<ul style="list-style-type: none"> <li>• MP-6, Media Sanitization</li> </ul>	
<b>Logical Access to Interfaces</b>			
1. Authentication Support	<ul style="list-style-type: none"> <li>• Ability for the IoT device to require authentication prior to connecting to the device</li> <li>• Ability for the IoT device to support a second, or more, authentication method(s) through an out-of-band path such as: Temporary passwords or other one-use credentials; Third-party credential checks; Biometrics; Text messages; Hard Tokens; etc.</li> <li>• Ability for the IoT device to hide or mask authentication information during the authentication process</li> </ul>	<ul style="list-style-type: none"> <li>• IA-2, Identification and Authentication</li> <li>• IA-6, Authenticator Feedback</li> </ul>	
2. Authentication Configuration	<ul style="list-style-type: none"> <li>• 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</li> <li>• Ability to disable or lock access to the device after an established number of unsuccessful login attempts</li> <li>• Ability to display and/or report the previous date and time of the last successful login following successful login authentication</li> </ul>	<ul style="list-style-type: none"> <li>• AC-7, Unsuccessful Logon Attempts</li> </ul>	

Sub-Capability	Key Abilities	Possible SP 800-53 Rev. 5 Controls Supported	Informative References
	<ul style="list-style-type: none"> <li>Ability to automatically disable accounts for the IoT device after an established period of inactivity.               <ul style="list-style-type: none"> <li>Ability to support automatic logout of inactive accounts after a configurable established time period.</li> <li>Ability to support automatic removal of temporary, emergency and other special use accounts after an established time period</li> </ul> </li> </ul>		
3. System Use Notification Support	<ul style="list-style-type: none"> <li>Ability to create an organizationally-defined system use notification message or banner to be displayed on the IoT device</li> <li>Ability to keep the notification message or banner on the device screen until the device user actively acknowledges and agrees to the usage conditions</li> </ul>	<ul style="list-style-type: none"> <li>AC-8, System Use Notification</li> </ul>	
4. Authorization Support	<ul style="list-style-type: none"> <li>Ability to identify authorized users and processes</li> <li>Ability to differentiate between authorized and unauthorized users (physical and remote)</li> </ul>	<ul style="list-style-type: none"> <li>IA-2, Identification and Authentication</li> </ul>	
5. Authentication & Identity Management	<ul style="list-style-type: none"> <li>Ability to establish access to the IoT device to perform organizationally-defined user actions without identification or authentication</li> </ul>	<ul style="list-style-type: none"> <li>AC-14, Permitted Actions Without Identification or Authentication</li> </ul>	
6. Role Support & Management	<ul style="list-style-type: none"> <li>Ability to create unique IoT device user accounts</li> <li>Ability to identify unique IoT device user accounts</li> <li>Ability to establish organizationally-defined user actions for accessing the IoT device and/or device interface</li> </ul>	<ul style="list-style-type: none"> <li>AC-2, Account Management</li> <li>IA-4, Identifier Management</li> <li>AC-3, Access Enforcement</li> </ul>	
7. Interface Control	<ul style="list-style-type: none"> <li>Ability to establish requirements for remote access to the IoT device and/or IoT device interface including:               <ul style="list-style-type: none"> <li>Usage restrictions</li> <li>Configuration requirements</li> <li>Connection requirements</li> <li>Manufacturer established requirement"</li> </ul> </li> <li>Ability to restrict use of IoT device components (e.g., ports, functions, microphones, video)</li> <li>Ability to logically or physically disable any local and network interfaces that are not necessary for the core functionality of the device</li> <li>Ability to restrict updating actions to authorized entities</li> <li>Ability to restrict access to the cybersecurity state indicator to authorized entities</li> <li>Ability to restrict use of IoT device services</li> <li>Ability to enforce the established local and remote access requirements</li> <li>Ability to support wireless technologies needed by the organization (e.g., Microwave, Packet radio (UHF/VHF), Bluetooth, Manufacturer defined)</li> <li>Ability to establish and configure IoT device settings for wireless technologies including wireless authentication protocols (e.g., EAP/TLS, PEAP)</li> </ul>	<ul style="list-style-type: none"> <li>AC-17 Remote Access</li> <li>CM-7, Least Functionality</li> <li>AC-3, Access Enforcement</li> <li>AC-18, Wireless Access</li> </ul>	

Sub-Capability	Key Abilities	Possible SP 800-53 Rev. 5 Controls Supported	Informative References
<b>Software Update</b>			
1. Update Application Support	<ul style="list-style-type: none"> <li>Ability to update the device's software through remote (e.g., network download) and/or local (e.g., removable media) means</li> <li>If software updates are delivered and applied automatically: <ul style="list-style-type: none"> <li>Ability to verify and authenticate any update before installing it</li> <li>Ability to enable or disable updating</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>SI-2, Flaw Remediation</li> </ul>	
<b>Cybersecurity State Awareness</b>			
1. Access to Event Information	<ul style="list-style-type: none"> <li>Ability to access information about the IoT device's cybersecurity state and other necessary data</li> <li>Ability to preserve system state information</li> </ul>	<ul style="list-style-type: none"> <li>SI-4, System Monitoring</li> <li>AU-12, Audit Record Generation</li> </ul>	
2. Event Identification & Monitoring	<ul style="list-style-type: none"> <li>Ability to identify organizationally-defined cybersecurity events (e.g., expected state change) that may occur on or involving the IoT device</li> <li>Ability to monitor for organizationally-defined cybersecurity events (e.g., expected state change) that may occur on or involving the IoT device</li> <li>Ability to support a list of events that are necessary for auditing purposes (to support organization's audit policy)</li> <li>Ability to identify unique users interacting with the device (to allow for user session monitoring)</li> <li>Ability to monitor communications traffic</li> <li>Ability to detect remote activation attempts</li> <li>Ability to detect remote activation of a collaborative computing device/component (e.g., microphone, camera)</li> <li>Ability to define characteristics of unapproved content</li> <li>Ability to scan files for unapproved content</li> </ul>	<ul style="list-style-type: none"> <li>SI-4, System Monitoring</li> <li>AU-2, Event Logging</li> <li>IA-2, Identification and Authentication</li> <li>SC-7, Boundary Protection</li> <li>SC-15, Collaborative Computing Devices and Applications</li> <li>CA-7, Continuous Monitoring</li> </ul>	
3. Event Response	<ul style="list-style-type: none"> <li>Ability to generate alerts for specific events</li> <li>Ability to respond to alerts with predefined responses</li> <li>Ability to alert connected information systems of potential issues found during the auditing process</li> <li>Ability to provide information to an external process that will issue auditing process alerts</li> <li>Ability to notify users of activation of a collaborative computing device</li> <li>Ability to respond following an auditing failure (either by the device or an external auditing process)</li> <li>Ability to prevent download of unapproved content</li> <li>Ability to delete unapproved content</li> </ul>	<ul style="list-style-type: none"> <li>SI-4, System Monitoring</li> <li>IR-4, Incident Handling</li> <li>AU-6, Audit Record Review, Analysis, and Reporting</li> <li>SC-15, Collaborative Computing Devices and Applications</li> <li>AU-5, Response to Audit Logging Process Failures</li> <li>RA-7 Risk Response</li> </ul>	
4. Logging Capture & Trigger Support	<ul style="list-style-type: none"> <li>Ability to identify and capture organizationally-defined events using a persistent method</li> <li>Ability to capture information from organizationally-defined cybersecurity events</li> </ul>	<ul style="list-style-type: none"> <li>AU-2, Event Logging</li> <li>AU-3, Content of Audit Records</li> </ul>	

Sub-Capability	Key Abilities	Possible SP 800-53 Rev. 5 Controls Supported	Informative References
	<p>(e.g., cybersecurity state, time) through organizationally-defined means (e.g., logs)</p> <ul style="list-style-type: none"> <li>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)</li> </ul>		
5. Support of Required Data Logging	<ul style="list-style-type: none"> <li>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</li> <li>Ability to log information pertaining to: <ul style="list-style-type: none"> <li>The type of event that occurred</li> <li>The time that the event occurred</li> <li>Where the event occurred</li> <li>The source of the event</li> <li>The outcome of the event</li> <li>Identity of users/processes associated with the event</li> </ul> </li> <li>Ability to provide information as to why the device captured a particular event or set of events</li> <li>Ability to capture organizationally-defined information to support examination of security incidents</li> <li>Ability to record stored data access and usage</li> </ul>	<ul style="list-style-type: none"> <li>AU-2, Event Logging</li> <li>AU-3, Content of Audit Records</li> </ul>	
6. Audit Log Storage & Retention	<ul style="list-style-type: none"> <li>Ability to comply with organizational policy for storing persistent audit logs up to a predefined size</li> <li>Ability to comply with organizational policy for audit log retention period</li> <li>Ability to delete audit logs in accordance with organizational policy</li> </ul>	<ul style="list-style-type: none"> <li>AU-4, Audit Log Storage Capacity</li> <li>AU-11, Audit Record Retention</li> </ul>	
7. Support for Reliable Time	<ul style="list-style-type: none"> <li>Ability to use synchronization with a verified time source to determine the validity of a timestamp</li> <li>Ability to record timestamps convertible to UTC or GMT to support a standardized representation of timing</li> <li>Ability to log timing measurements outside a threshold value (e.g., enabling alerts if device's system time is not reliable)</li> </ul>	<ul style="list-style-type: none"> <li>AU-8, Time Stamps</li> </ul>	
8. Audit Support & Protection	<ul style="list-style-type: none"> <li>Ability to report on its cybersecurity state</li> <li>Ability to support a self-audit generation process</li> <li>Ability to send requested audit logs to an external audit process or information system (e.g., where audit information can be checked to allow for review, analysis, and reporting.)</li> <li>Ability to protect the audit information through the use of: <ul style="list-style-type: none"> <li>Encryption</li> <li>Digitally signing audit files</li> <li>Securely sending audit files to another device</li> <li>Other protections created by the device manufacturer</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>SI-4, System Monitoring</li> <li>AU-6, Audit Record Review, Analysis, And Reporting</li> <li>AU-9, Protection of Audit Information</li> </ul>	



Sub-Capability	Key Abilities	Possible SP 800-53 Rev. 5 Controls Supported	Informative References
9. State Awareness Support	<ul style="list-style-type: none"> <li>Ability to differentiate between when a device will likely operate as expected from when it may be in a degraded cybersecurity state</li> </ul>	<ul style="list-style-type: none"> <li>SI-5, Security Alerts, Advisories, and Directives</li> </ul>	
<b>Device Security</b>			
1. Secure Execution	<ul style="list-style-type: none"> <li>Ability to execute code in confined virtual environments</li> <li>Ability to separate IoT device processes into separate execution domains</li> </ul>	<ul style="list-style-type: none"> <li>SC-39, Process Isolation</li> </ul>	
2. Secure Communication	<ul style="list-style-type: none"> <li>Ability to enforce traffic flow policies</li> <li>Ability to interface with DNS/DNSSEC</li> </ul>	<ul style="list-style-type: none"> <li>SC-21, Secure Name/Address Resolution Service</li> </ul>	
3. Secure Resource Usage	<ul style="list-style-type: none"> <li>Ability to manage memory address space assigned to processes</li> <li>Ability to enforce access to memory space through the kernel</li> <li>Ability to prevent a process from accessing memory space of another process</li> <li>Ability to enforce configured disk quotas</li> <li>Ability to utilize file compression technologies (e.g., to provide denial of service protection)</li> </ul>	<ul style="list-style-type: none"> <li>SC-39, Process Isolation</li> <li>SC-5, Denial of Service Protection</li> </ul>	
4. Secure Device Operation	<ul style="list-style-type: none"> <li>Ability to define various operational states</li> <li>Ability to restrict components/features of the IoT device (e.g., ports, functions, protocols, services) in accordance with organizationally-defined policies</li> </ul>	<ul style="list-style-type: none"> <li>CP-10, System Recovery and Reconstitution</li> <li>SC-24, Fail in Known State<sup>11</sup></li> <li>CM-7, Least Functionality</li> <li>CP-12, Safe Mode</li> </ul>	

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 in the Federal Profile**

Sub-Capability	Key Actions	Primary SP 800-53 Rev. 5 Controls Supported	Informative References
<b>Documentation</b>			
1. Device Acquisition and	<ul style="list-style-type: none"> <li>Document all the IoT device security and privacy capabilities and limitations details.</li> </ul>	<ul style="list-style-type: none"> <li>MA-1, Policy and Procedures</li> </ul>	

<sup>11</sup> While SC-24 is not in the low baseline, it is important for many IoT devices in that the device has to fail in a state that still preserves critical functionality. For example, the connected refrigerator still has to stay cold, and the connected smoke alarm still has to function as an auditory smoke alarm even if the connection fails.

Sub-Capability	Key Actions	Primary SP 800-53 Rev. 5 Controls Supported	Informative References
Maintenance Planning Support	<ul style="list-style-type: none"> <li>• Document information necessary to inform the review and update of the IoT device systems, and the services' acquisition practices by IoT device customers.</li> <li>• Document all anticipated costs associated with the IoT device, including the purchase, maintenance, operations, security, and disposal costs throughout the potential lifetime of the use of the IoT device.</li> <li>• Document the type and nature of the local and/or remote maintenance activities required once the IoT device is purchased and deployed in the organization.</li> <li>• Document the physical requirements, operational requirements, technical capabilities, and other related issues, required to sufficiently support all maintenance activities.</li> <li>• Document the type and nature of the remote maintenance and diagnostic activities required by the manufacturer once the device is purchased and deployed in the IoT customer organization.</li> <li>• Document the physical and technical capabilities required to support the IoT device maintenance and diagnostic activities.</li> <li>• Document the type and nature of the local and/or remote maintenance activities required, including those that will involve and require manufacturer personnel or their contractors to access the IoT device, once the device is purchased and deployed.</li> <li>• Document the specific maintenance requirements and associated procedures and/or instructions for defined maintenance tasks that must be performed by IoT device customers, and by manufacturer's personnel.</li> <li>• Document the events that will trigger IoT device system review and maintenance by the IoT device customer, and the suggested frequency of system review and maintenance activities for IoT devices.</li> </ul>	<ul style="list-style-type: none"> <li>• MA-4, Nonlocal Maintenance</li> <li>• MA-5, Maintenance Personnel</li> <li>• PM-3, Information Security and Privacy Resources</li> <li>• SA-1, Policy and Procedures</li> <li>• SA-2, Allocation of Resources</li> <li>• SA-4, Acquisition Process</li> <li>• SI-4, System Monitoring</li> </ul>	
2. Legal & Regulatory Compliance Support	<ul style="list-style-type: none"> <li>• Document all security standards requirements, such as SP 800-53 Rev 5 controls, ISO security and/or privacy standards controls, etc., that are used to support security and privacy regulatory requirements with which the IoT device capabilities must comply within the IoT device customer's information systems.</li> <li>• Document the legal security and privacy controls requirements (Federal regulations, international regulations, state and local laws) for which the IoT device has capabilities that support compliance. Some examples: Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA), EU General Data Protection Regulation (GDPR).</li> </ul>	<ul style="list-style-type: none"> <li>• SI-1, Policy and Procedures</li> <li>• PM-27, Privacy Reporting</li> </ul>	

Sub-Capability	Key Actions	Primary SP 800-53 Rev. 5 Controls Supported	Informative References
3. Continuous Monitoring Support	<ul style="list-style-type: none"> <li>Document all the ways in which the IoT device can be monitored along with recommended associated tools to perform monitoring.</li> <li>Document IoT device behavior and known indicators of attacks being launched on the IoT device.</li> <li>Describe how to identify local, network and remote IoT device access attempts and connections.</li> <li>Describe expected behavior of the normal operation of the IoT device.</li> </ul>	<ul style="list-style-type: none"> <li>CA-7, Continuous Monitoring</li> </ul>	
4. Documentation for Device Cybersecurity Capabilities	<ul style="list-style-type: none"> <li>Document information about capabilities within the IoT device that allow for unique identification of each IoT device.</li> <li>Document the configuration settings available within the IoT device, those that are recommended as minimum required configuration settings, and the explanation for being minimum required settings.</li> <li>Document information about how to use the IoT device capabilities to irreversibly remove all data from the device.</li> <li>Document 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, in ways that support applicable legal requirements for monitoring.</li> <li>Document the manufacturer needs for access to the IoT device interfaces for support, updates, ongoing maintenance, etc.</li> <li>Document the manufacturer requirements for data collection from the device.</li> <li>Document the types of access to the IoT device the manufacturer will require on an ongoing and/or regular basis.</li> <li>Document the role-based access capabilities built within the device, such as admin, general user, etc.</li> <li>Document the IoT device's logical and remote interface access controls capabilities.</li> </ul>	<ul style="list-style-type: none"> <li>AC-1, Policy and Procedures</li> <li>CM-1, Policies and Procedures</li> <li>CM-2, Baseline Configuration</li> <li>IA-4, Identifier Management</li> <li>PM-20, Dissemination of Privacy Program Information</li> <li>PS-6, Access Agreements</li> <li>SA-4, Acquisition Process</li> <li>SI-4, System Monitoring</li> <li>SI-12, Information Management and Retention</li> </ul>	
5. Documentation for Post-Market Customer Activities	<ul style="list-style-type: none"> <li>Document how to configure the IoT devices, and related actions to take with the devices.</li> <li>Document the process and detailed instructions for backing up data on the IoT device.</li> <li>Provide documented instructions for implementing and using the unique IoT identifiers.</li> <li>Document instructions for restricting interface connections that enable specific activities on the device.</li> <li>Document the device interface controls in detail, and the support provided for implementing a second factor for authentication. If multi-factor authentication is not possible, then document that this is not a capability of the IoT device.</li> <li>Document how to configure the IoT device to technically support PIV implementation, accessibility and interfaces.</li> </ul>	<ul style="list-style-type: none"> <li>AC-1, Policy and Procedures</li> <li>AC-2, Account Management</li> <li>AU-9, Protection of Audit Information</li> <li>CM-1, Policies and Procedures</li> <li>CM-2, Baseline Configuration</li> <li>CP-9, System Backup</li> <li>IA-1, Policy and Procedures</li> <li>IA-2, Identification and Authentication</li> </ul>	

Sub-Capability	Key Actions	Primary SP 800-53 Rev. 5 Controls Supported	Informative References
	<ul style="list-style-type: none"> <li>Document how to integrate the device with a PIV system. And/or, as acceptable by the IoT customer, provide an attestation that the device can comply with Federal agency requirements, along with providing associated descriptions for how the agency can accomplish this.</li> <li>Document the indicators of unauthorized use of the IoT device.</li> <li>Document the types of usage and environmental systems data that can be collected from the IoT device.</li> <li>Document the IoT device security capabilities, security strength capabilities, and security assurance capabilities.</li> <li>Document the recommended device roles and responsibilities to support the ability for IoT device customers to determine to what level in their hierarchy of privileges that the documentation pertains.</li> </ul>	<ul style="list-style-type: none"> <li>IA-4, Identifier Management</li> <li>PL-4, Rules of Behavior</li> <li>PM-20, Dissemination of Privacy Program Information</li> <li>PS-6, Access Agreements</li> <li>SI-4, System Monitoring</li> <li>SA-5, System Documentation</li> </ul>	
<b>Information and Query Reception</b>			
1. Cybersecurity Feature Reports and Queries	<ul style="list-style-type: none"> <li>Document the process by which IoT device customers can contact the manufacturer to ask questions or obtain help related to the minimum requirements for the IoT device configuration settings.</li> <li>Document directions and procedures for how IoT customers should submit questions and requests for information about IoT device security and privacy compliance requirements. Some examples: Federal Information Security Modernization Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA), EU General Data Protection Regulation (GDPR).</li> <li>Document instructions for reporting/sending the manufacturer IoT device flaw reports.</li> <li>Document manufacturer's procedures for processing the flaw reports, determining which flaws need to be fixed, how the manufacturer will correct the flaws, and any actions the customer may need to take to correct identified flaws.</li> <li>Document procedures IoT customers need to follow to receive IoT device remediation reports from manufacturers.</li> <li>If the IoT device manufacturer provides anti-malware tools for the associated IoT device, or if the IoT device has built-in anti-malware capabilities, document procedures for the IoT device customer to respond to and report false positives to the manufacturer.</li> </ul>	<ul style="list-style-type: none"> <li>AC-1, Policy and Procedures</li> <li>CM-1, Policies and Procedures</li> <li>CM-2, Baseline Configuration</li> <li>PM-20, Dissemination of Privacy Program Information</li> <li>SI-2, Flaw Remediation</li> <li>SI-3, Malicious Code Protection</li> </ul>	
<b>Information Dissemination</b>			
1. Cybersecurity and Vulnerability Alerts	<ul style="list-style-type: none"> <li>Document the processes the manufacturer will follow to communicate their IoT device remediation efforts to their stakeholders (IoT device customers, users, etc.).</li> </ul>	<ul style="list-style-type: none"> <li>CM-4, Impact Analyses</li> </ul>	

Sub-Capability	Key Actions	Primary SP 800-53 Rev. 5 Controls Supported	Informative References
	<ul style="list-style-type: none"> <li>• Document newly identified flaws and vulnerabilities for the associated IoT devices.</li> <li>• Document the anti-malware recommendations. If no anti-malware is needed for the IoT device, explain why.</li> <li>• Document the IoT device resource constraints for malicious code protection, and possible compensating controls that IoT device customers can use for such constraints.</li> <li>• Document a procedure to communicate information about cybersecurity incidents involving the IoT device to IoT device customers.</li> <li>• Document manufacturer's device flaw remediation efforts with stakeholders and IoT device customers.</li> </ul>	<ul style="list-style-type: none"> <li>• IR-1, Incident Response Policies and Procedures</li> <li>• MA-1, Policy and Procedures</li> <li>• SA-5, System Documentation</li> <li>• SI-2, Flaw Remediation</li> <li>• SI-3, Malicious Code Protection</li> </ul>	
2. Software Update and Maintenance Notification	<ul style="list-style-type: none"> <li>• Document IoT device security updates and privacy considerations, 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.</li> <li>• Document instructions for IoT device customers to follow to review and update as necessary their IoT device systems and services practices, policies, and procedures.</li> <li>• Document IoT device maintenance operations performed by the manufacturer. Document instructions for how IoT device customers must perform device maintenance operations themselves if the manufacturer does not offer comprehensive IoT device maintenance operations.</li> </ul>	<ul style="list-style-type: none"> <li>• MA-2, Controlled Maintenance</li> <li>• SI-5, Security Alerts, Advisories, and Directives</li> </ul>	
<b>Education and Awareness</b>			
1. Device Support Awareness	<ul style="list-style-type: none"> <li>• Document the means (tools, assistance, instructions, etc.) to establish distinct roles with a hierarchy of privileges within the IoT device (for example, the ability to assign read-only access to device data for auditors versus full access to the device for system admins).</li> <li>• Document the means (tools, assistance, instructions, etc.) to enable the IoT device to support audit and log maintenance and repairs operations. Document the specific maintenance procedures for defined maintenance tasks.</li> <li>• Document and provide training materials to ensure IoT device customers understand the requirements for specified maintenance procedures.</li> <li>• Document and provide training materials to IoT device customers to ensure they understand the manufacturer's cybersecurity incident response procedures and their associated involvement, if any.</li> <li>• Document and provide training materials to IoT device customers to ensure they understand the requirements for specified maintenance procedures.</li> </ul>	<ul style="list-style-type: none"> <li>• IR-2, Incident Response Training</li> <li>• MA-1, Policy and Procedures</li> <li>• MA-5, Maintenance Personnel</li> <li>• PL-1, Policy and Procedures</li> </ul>	

Sub-Capability	Key Actions	Primary SP 800-53 Rev. 5 Controls Supported	Informative References
2. Device Cybersecurity Capability Awareness	<ul style="list-style-type: none"> <li>• Document detailed instructions (e.g., using training videos, webinars, written directions) for implementing and using IoT device unique identifiers.</li> <li>• Document detailed instructions and/or training detailing how to configure the IoT device, change configuration settings and perform related actions to meet their customers' needs and requirements.</li> <li>• Document clear instructions and/or demonstrate (e.g., directly in person, in videos, in an online webinar) how to backup up the IoT device.</li> <li>• Document clear instructions, descriptions, and/or training for how to use the IoT device data removal capabilities and procedures.</li> <li>• Document instructions for how to establish and change role-based access settings. If role-based access capabilities are not available, document the limitation.</li> <li>• Document the types of security and privacy tests necessary for the IoT device and software before installation.</li> <li>• If the IoT device manufacturer provides anti-malware for the associated IoT device, or if the IoT device has built-in anti-malware capabilities, document instructions for how to perform real-time scanning for new files introduced through the IoT device interfaces and how to schedule automatic scanning on the IoT device.</li> <li>• If the IoT device manufacturer provides anti-malware for the associated IoT device, or if the IoT device has built-in anti-malware capabilities, document instructions for how to configure the IoT device to shut-down upon detecting malicious code, as appropriate to the purpose of the IoT device, and for how to block and/or quarantine malicious code to allow for inspection of that code by customer organizational roles with those responsibilities.</li> <li>• Document the operational impacts of the anti-malware activities on mission critical processes in the system where the IoT device is used. Provide additional information on recommended responses to malware beyond just shutting down the IoT device.</li> <li>• Document options for responding to malicious code identification within the IoT device. Some examples of options include, but are not limited to: shutting down, redirecting the network traffic, sending alerts, logging the events, etc.</li> <li>• If the IoT device manufacturer provides anti-malware tools for the associated IoT device, or if the IoT device has built-in anti-malware capabilities, document the possible availability and functioning impacts on the associated IoT device and the system within which it is implemented.</li> </ul>	<ul style="list-style-type: none"> <li>• AT-3, Role-based Training</li> <li>• CA-7, Continuous Monitoring</li> <li>• CM-1, Policies and Procedures</li> <li>• CM-2, Baseline Configuration</li> <li>• CM-4, Impact Analyses</li> <li>• CP-9, System Backup</li> <li>• IA-4, Identifier Management</li> <li>• PM-20, Dissemination of Privacy Program Information</li> <li>• SI-3, Malicious Code Protection</li> <li>• SI-12, Information Management and Retention</li> </ul>	

Sub-Capability	Key Actions	Primary SP 800-53 Rev. 5 Controls Supported	Informative References
	<ul style="list-style-type: none"><li>• Document how to best implement and secure the IoT device and associated systems monitoring capabilities.</li></ul>		

344

### 3 Conclusion

The federal profile using the IoT core baseline and non-technical baseline is a helpful starting point for both manufacturers and organizations to identify pertinent device cybersecurity requirements (e.g., device cybersecurity capabilities and non-technical supporting capabilities) needed to support system and organizational security goals. The capabilities included in the profile are meant to represent those commonly needed by organizations to incorporate a device into a system of low-impact (i.e., an information system that is determined to be of a low risk impact based on a risk assessment). 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.

In other cases, 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. 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. Additionally, 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.

With these limitations in mind, organizations and manufacturers can use the federal profile as a starting point to anticipate device cybersecurity and non-technical supporting capabilities needed from and related to IoT devices. These limitations also mean that organizations and manufacturers should work together wherever possible to identify device cybersecurity requirements that apply to more specific organizations and use cases. Manufacturers and customers should also be aware that all use cases cannot be predicted, especially for IoT devices where one device could offer many uses. Manufacturers providing robust non-technical support, including the kinds of documentation, actions, and other concepts discussed in this publication will enable a wide range of customers to securely use a device.



372 **References**

- [1] 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>
- [2] Fagan M, Marron J, Brady KG Jr., Cuthill BB, Megas KN, Herold R (2020) IoT Device Cybersecurity Guidance for the Federal Government: An Approach for Establishing IoT Device Cybersecurity Requirements. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (SP) 800-213. Available [when released] at <https://doi.org/10.6028/NIST.SP.800-213-draft>
- [3] 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>
- [4] Fagan M, Marron J, Brady KG, Jr, Cuthill BB, Megas KN, Herold R (2020) IoT Non-Technical Supporting Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Interagency or Internal Report (IR) 8259B. <https://doi.org/10.6028/NIST.IR.8259B-draft>
- [5] Fagan M, Marron, J, Brady KG, Jr, Cuthill BB, Megas KN, Herold R (2020) Creating a Profile Using the IoT Core Baseline and non-technical baseline. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Interagency or Internal Report (IR) 8259C. <https://doi.org/10.6028/NIST.IR.8259C-draft>
- [6] Subrahmanian E, Rachuri S, Bouras A, Fenves SJ, Foufou S, Sriram RD (2006) The Role of Standards in Product Lifecycle Management Support. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7289. <https://doi.org/10.6028/NIST.IR.7289>
- [7] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. <https://doi.org/10.6028/NIST.SP.800-53r5>
- [8] National Institute of Standards and Technology (2020) IoT Device Cybersecurity Requirement Catalogs. (National Institute of Standards and Technology, Gaithersburg, MD). Available at <https://pages.nist.gov/FederalProfile-8259A/>
- [9] Joint Task Force Transformation Initiative (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>
- [10] Cyber-Physical Systems Public Working Group (2017) Framework for Cyber-Physical Systems: Volume 1, Overview, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1500-201. <https://doi.org/10.6028/NIST.SP.1500-201>

- [11] Johnson A, Dempsey K, Ross R, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128. <https://doi.org/10.6028/NIST.SP.800-128>
- [12] International Organization for Standardization (ISO) 9000:2015, Quality management systems – Fundamentals and vocabulary, September 2015.
- [13] Barker E, Chen L, Roginsky A, Vassilev A, Davis R (2019) Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56A, Rev. 3. <https://doi.org/10.6028/NIST.SP.800-56Ar3>
- [14] Committee on National Security Systems (2015) Committee on National Security Systems (CNSS) Glossary. (National Security Agency, Ft. Meade, MD), CNSS Instruction (CNSSI) No. 4009. Available at <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>
- [15] Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 2. <https://doi.org/10.6028/NIST.SP.800-82r2>
- [16] Souppaya M, Scarfone K (2013) Guide to Enterprise Patch Management Technologies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 3. <https://doi.org/10.6028/NIST.SP.800-40r3>

**Appendix A—Acronyms**

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

ACD	Applied Cybersecurity Division
CSF	Cybersecurity Framework
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
EAP	Extensible Authentication Protocol
FISMA	Federal Information System Modernization Act
GDPR	General Data Protection Regulation
GMT	Greenwich Mean Time
HIPAA	Health Insurance Portability and Accountability Act
ICS	Industrial Control Systems
IoT	Internet of Things
ITL	Information Technology Laboratory
IR	Internal Report
MAC	Media Access Control
NIST	National Institute of Standards and Technology
PEAP	Protected Extensible Authentication Protocol
RMF	Risk Management Framework
SP	Special Publication
TLS	Transport Layer Security
UHF	Ultra-High Frequency
UTC	Coordinated Universal Time
VHF	Very High Frequency

398 **Appendix B—Glossary**

399 Selected terms used in this document are defined below.

Authorized Entity	An entity that has implicitly or explicitly been granted approval to interact with a particular IoT device. The device cybersecurity capabilities in the core baseline do not specify how authorization is implemented for distinguishing authorized and unauthorized entities, but can include identity management and authentication to establish the authorization of entities. It is left to the organization to decide how each device will implement authorization. Also, an entity authorized to interact with an IoT device in one way might not be authorized to interact with the same device in another way.
Configuration [11, Adapted]	The possible conditions, parameters, and specifications with which an information system or system component can be described or arranged. The Device Configuration capability does not define which configuration settings should exist, simply that a mechanism to manage configuration settings exists.
Core Baseline	A set of technical device capabilities needed to support common cybersecurity controls that protect the customer's devices and device data, systems, and ecosystems.
Customer [12]	The organization or person that receives a product or service.
Cybersecurity State	The condition of a device's cybersecurity expressed in a way that is meaningful and useful to authorized entities. For example, a very simple device might express its state in terms of whether or not it is operating as expected, while a complex device might perform cybersecurity logging, check its integrity at boot and report the results, and examine and report additional aspects of its cybersecurity state.
Device Cybersecurity Capability	Cybersecurity features or functions that computing devices provide through their own technical means (i.e., device hardware and software).
Degraded Cybersecurity State	A cybersecurity state that indicates the device's cybersecurity has been significantly negatively impacted, such as the device being unable to operate as expected, or the integrity of the device's software being violated.
Device Cybersecurity Capability Core Baseline	See <i>core baseline</i> .

Device Identifier [13, Adapted]	A context-unique value—a value unique within a specific context—that is associated with a device (for example, a string consisting of a network address).
Entity	A person, device, service, network, domain, manufacturer, or other party who might interact with an IoT device.
Federal Profile	Profile of the IoT device cybersecurity capability core baseline [3] and non-technical supporting capability core baseline [4] to provide security guidance provided to federal government organizations related to IoT devices.
Interface [14, Adapted]	A boundary between the IoT device and entities where interactions take place. There are two types of interfaces: network and local.
Local Interface	An interface that can only be accessed physically, such as a port (e.g., USB, audio, video/display, serial, parallel, Thunderbolt) or a removable media drive (e.g., CD/DVD drive, memory card slot).
Logical Identifier	A device identifier that is expressed logically by the device's software. An example is a media access control (MAC) address assigned to a network interface.
Maintenance [15]	Any act that either prevents the failure or malfunction of IoT device and supporting equipment or restores its operating capability.
Network Interface	An interface that connects the IoT device to a network.
Non-Technical Supporting Capability	Non-technical supporting capabilities are actions an organization performs in support of the cybersecurity of an IoT device.
Non-Technical Supporting Capability Core Baseline	The non-technical supporting capability core baseline is a set of non-technical supporting capabilities generally needed from manufacturers or other third parties to support common cybersecurity controls that protect an organization's devices as well as device data, systems, and ecosystems.
Physical Identifier	A device identifier that is expressed physically by the device (e.g., printed onto a device's housing, displayed on a device's screen).

Profile	A profile is a baseline set of minimal cybersecurity requirements for mitigating described threats and vulnerabilities, as well as supporting compliance requirements for a defined scope and type of a particular use case (e.g., industry, information system(s)), using a combination of existing cybersecurity guidance, standards and/or specifications baseline documents or catalogs. A profile organizes selected guidance, standard(s) and/or specification(s) and may narrow, expand and/or otherwise tailor items from the starting material to address the requirements of the profile's target application.
Software [7]	Computer programs and associated data that may be dynamically written or modified during the device's execution (e.g., application code, libraries).
Supporting Parties	Providers of external system services to the manufacturer through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. Supporting services include, for example, Telecommunications, engineering services, power, water, software, tech support, and security.
Term of Support	The length of time for which the device will be supported by the manufacturer or supporting parties for such actions and materials as part replacements, software updates, vulnerability notices, technical support questions, etc.
Training	Teaching people the knowledge and relevant and needed security skills and competencies by that will enable them to understand how to use and configure the IoT devices to enable them to most securely use the IoT devices.
Update [16, Adapted]	A patch, upgrade, or other modification to code that corrects security and/or functionality problems in software.