Draft NISTIR 8259D

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

NIST

**National Institute of
Standards and Technology**

U.S. Department of Commerce

21 **Draft NISTIR 8259D**

22

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

December 2020

76 **Reports on Computer Systems Technology**

85 **Abstract**

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

94 **Keywords**

97 **Acknowledgments**

105 **Audience**

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

109

Note to Reviewers

110

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

116   • **NISTIR 8259:** *Foundational Cybersecurity Activities for IoT Device Manufacturers*
117   • **NISTIR 8259A:** *IoT Device Cybersecurity Capability Core Baseline*
118

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

122   • *NISTIR 8259B: IoT Non-technical and Supporting Capability Core Baseline* – NISTIR
123   8259B complements the NISTIR 8259A device cybersecurity core baseline by detailing
124   what additional, non-technical support is typically needed from manufacturers. This non-
125   technical baseline collects and makes explicit support capabilities like documentation,
126   training support, etc.
127   • *NISTIR 8259C: Creating a Profile of the IoT Core Baseline and Non-Technical*
128   *Baseline* – NISTIR 8259C presents a method of profiling the baselines in NISTIR 8259A
129   and NISTIR 8259B to create a more detailed set of capabilities responding to the
130   concerns of a specific sector, based on some authoritative source such as a standard or
131   other guidance. This is the method used to create the profile meeting the requirements of
132   the federal information system low baseline.
133   • *NISTIR 8259D: Profile Using the IoT Core Baseline and Non-Technical Baseline for*
134   *the Federal Government* – NISTIR 8259D presents the profile defining the capabilities
135   needed from and related to IoT devices to incorporate those devices into a federal
136   information system implementing the low baseline controls of NIST SP 800-53.
137

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

146   NIST appreciates all comments, concerns and identification of areas needing clarification.
147   Ongoing discussion with the stakeholder community is welcome as we work to improve the
148   cybersecurity of IoT devices. **Community input is specifically sought regarding the mapping**
149   **of specific reference document content to the items in Tables 1 and 2, to populate the fourth**
150   **column, "IoT Reference Examples," to strongly align the NISTIR 8259D profile to the**
151   **existing body of cybersecurity guidance. Table 1 in NISTIR 8259A can be used as a model**
152   **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
186

187

Table of Contents

194

List of Appendices

198

List of Figures

202

List of Tables

206

207 **1   Introduction**

208   Many organizations[1] within the federal government are looking to acquire IoT devices. In many
209   cases, these IoT devices will act as elements of larger systems[2]. As such, the ability for an
210   organization to support the security[3] requirements of the associated system as well as those of
211   the organization is often dependent on the capabilities offered by the IoT device and/or the
212   manufacturer or affiliated third parties. IoT devices support these system and organizational
213   security requirements by providing both technical (device cybersecurity) capabilities and non-
214   technical (administrative and physical actions) supporting capabilities. As shown in Figure 1,
215   these IoT device cybersecurity capabilities and non-technical supporting capabilities enable
216   federal agencies to produce cybersecurity capabilities in their systems and organizations.
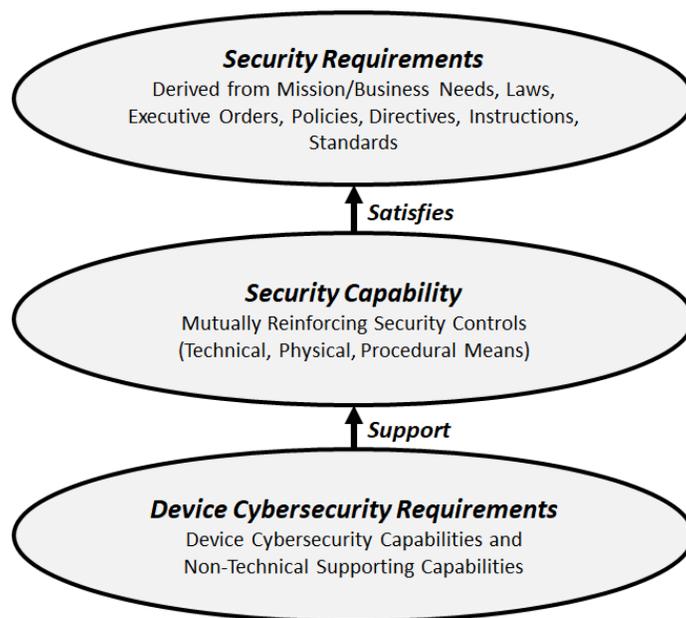
217

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

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

---

1   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.
2   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.
3   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.

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

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

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

252   This publication is best understood within the context provided by NISTIR 8259, NISTIR
253   8259A, *IoT Device Cybersecurity Capability Core Baseline* [3], NISTIR 8259B, *IoT Non-*
254   *Technical Supporting Capability Core Baseline* [4], and NISTIR 8259C, *Creating a Profile*
255   *Using the IoT Core Baseline and Non-Technical Baseline* [5]. The 8259 series aims to help
256   manufacturers understand how they play a role in their customers' cybersecurity. The IoT device

---

[4]   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].
[5]   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.

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

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

---

[6]   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].
[7]   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.
[8]   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.

273 **2   The Profile Using the IoT Core Baseline and Non-Technical Baseline for the**
274 **   Federal Government**

275 The following profile[9] (referred to as the federal profile) of the IoT device cybersecurity
276 capability core baseline and non-technical supporting capability core baseline was created using
277 the security guidance provided to federal government organizations and non-federal users (i.e.,
278 NIST SP 800-53 Rev. 5 and the Cybersecurity Framework [10]). The first step was to elaborate
279 on the core baseline and non-technical baseline with a catalog[10] of device-centric, cybersecurity-
280 focused capabilities that may be needed by federal government organizations to implement
281 cybersecurity capabilities. Using the controls from the low-impact RMF baseline from SP 800-
282 53B as guidance, device cybersecurity capabilities and non-technical supporting capabilities
283 were selected from the catalog for inclusion in the federal profile. The low impact baseline
284 provides a useful guide of minimal securability for the federal government and a starting point
285 for the federal profile. The core baseline, non-technical baseline, and other well-documented
286 concerns were also useful in defining the federal profile.

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

297 The federal profile is presented in two tables. Table 1 details the device cybersecurity capability
298 abilities in the federal profile. Table 2 details the non-technical supporting capability actions in
299 the federal profile. Each row in each table represents one *sub-capability*, which is a collection of
300 abilities or actions that redefine, expand, and/or specify the core capabilities from the IoT core
301 baseline using additional context from the sector and/or use case. These are grouped into seven
302 core IoT technical capabilities that manufacturers may have to design and build into IoT devices:
303 Device Identity, Device Configuration, Data Protection, Logical Access to Interfaces, Software
304 Update, Cybersecurity State Awareness, and Device Security. A group of sub-capabilities are all
305 related to their associated core capability but may or may not relate to each other. Similarly,
306 abilities or actions within a sub-capability all relate to the sub-capability but not necessarily to
307 each other. The arrangement of abilities or actions into sub-capabilities in the federal profile is
308 not meant to represent a formal definition of sub-capabilities, and other users of this profile or
309 creators of other profiles may arrange abilities and actions into sub-capabilities that are most

---

[9]   For clarification of the specific use of the term profile, see definition of "profile" or "federal profile" in the glossary.

[10]   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 [8].

310   meaningful for their organization, sector, and/or use case. For the federal profile, sub-capabilities
311   are grouped such that they reflect support for a specific control or approach to enable easier
312   tailoring of this profile for specific organizations. Sub-capabilities are described by:

313   •   First column: the name of the sub-capability. Related sub-capabilities commonly have
314   similar or standard names. **Please Note:** sub-capabilities are numbered for reference
315   purposes, and the assignment of numerals is not reflective of an explicit or implied
316   ordering of sub-capabilities.
317   •   Second column: the key abilities/actions of the sub-capability—aspects of the sub-
318   capability that are key to defining the sub-capability and supporting cybersecurity needs
319   and goals. For device cybersecurity capabilities, these are called *abilities*, referring to the
320   abilities of the device, while for non-technical supporting capabilities, these are called
321   *actions*, referring to actions taken by the manufacturer or third party.
322   •   Third column: the primary SP 800-53 Rev. 5 controls possibly supported (based upon
323   use case) by the sub-capability. This sub-capability is necessary based upon the context
324   for how the IoT device is used and the associated risk, but may not be sufficient by itself
325   to implement the control for a device. For example, there may need to be a capability for
326   the device to have an identifier to implement the control *AU-3 Content of Audit Records*
327   to support audit system logging of information about the device.
328   •   Fourth columns: reference examples to external guidance that provide more information
329   about the sub-capability. **Please Note:** this column is blank for the Public Comment draft
330   as NIST looks to the public for recommended informative references for the proposed
331   federal profile.

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

335   **Table 1 - Device Cybersecurity Capabilities in the Federal Profile**

Sub-Capability	Key Abilities	Possible SP 800-53 Rev. 5 Controls Supported	Informative References
Device Identity			
1. Identifier Management Support	• 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)	• IA-4, Identifier Management	
2. Actions Based on Device Identity	• Ability to monitor specific actions based on the IoT device identity • Ability to identify software loaded on the IoT device based on IoT device identity	• AU-3, Content of Audit Records • CM-8, System Component Inventory	
3. Physical Identifiers	• Ability to add a unique physical identifier at an external or internal location on the device authorized entities can access	• MP-4 Media Storage • PE-22 Component Marking	
Device Configuration			

Sub-Capability	Key Abilities	Possible SP 800-53 Rev. 5 Controls Supported	Informative References
1. Display Configuration	• Ability to configure content to be displayed on a device	• AC-8, System Use Notification	

2. Device Configuration Control	• Ability to change the device's software configuration settings
	• Ability for authorized entities to restore the device to a secure configuration defined by an authorized entity
	• Configuration settings for use with the Device Configuration capability including, but not limited to:
	  o Ability for authorized entities to configure the cryptography use itself, such as choosing a key length
	  o Ability to configure any remote update mechanisms to be either automatically or manually initiated for update downloads and installations
	  o Ability to enable or disable notification when an update is available and specify who or what is to be notified
		• CM-2, Baseline Configuration
		• CM-3, Configuration Change Control
		• CM-6, Configuration Settings	

Data Protection			
1. Cryptographic Capabilities & Support	• Ability to execute cryptographic mechanisms of appropriate strength and performance • Ability to verify digital signatures • Ability to run hashing algorithms • Ability to compute and compare hashes	• SC-13, Cryptographic Protection	
2. Cryptographic Key Management	• Ability to change keys securely • Ability to generate key pairs • Ability to store encryption keys securely	• SC-12, Cryptographic Key Establishment and Management	
3. Secure Storage	• Ability to "sanitize" or "purge" specific or all data in the device	• MP-6, Media Sanitization	
Logical Access to Interfaces			
1. Authentication Support	• Ability for the IoT device to require authentication prior to connecting to the device • 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. • Ability for the IoT device to hide or mask authentication information during the authentication process	• IA-2, Identification and Authentication • IA-6, Authenticator Feedback	
2. Authentication Configuration	• 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 • Ability to disable or lock access to the device after an established number of unsuccessful login attempts • Ability to display and/or report the previous date and time of the last successful login following successful login authentication	• AC-7, Unsuccessful Logon Attempts	

Sub-Capability	Key Abilities	Possible SP 800-53 Rev. 5 Controls Supported	Informative References

	• Ability to automatically disable accounts for the IoT device after an established period of inactivity.
	  ○ Ability to support automatic logout of inactive accounts after a configurable established time period.
	  ○ Ability to support automatic removal of temporary, emergency and other special use accounts after an established time period		

3. System Use Notification Support	• Ability to create an organizationally-defined system use notification message or banner to be displayed on the IoT device • Ability to keep the notification message or banner on the device screen until the device user actively acknowledges and agrees to the usage conditions	• AC-8, System Use Notification	
4. Authorization Support	• Ability to identify authorized users and processes • Ability to differentiate between authorized and unauthorized users (physical and remote)	• IA-2, Identification and Authentication	
5. Authentication & Identity Management	• Ability to establish access to the IoT device to perform organizationally-defined user actions without identification or authentication	• AC-14, Permitted Actions Without Identification or Authentication	
6. Role Support & Management	• Ability to create unique IoT device user accounts • Ability to identify unique IoT device user accounts • Ability to establish organizationally-defined user actions for accessing the IoT device and/or device interface	• AC-2, Account Management • IA-4, Identifier Management • AC-3, Access Enforcement	

7. Interface Control	• Ability to establish requirements for remote access to the IoT device and/or IoT device interface including:
	  ○ Usage restrictions
	  ○ Configuration requirements
	  ○ Connection requirements
	  ○ Manufacturer established requirement"
	• Ability to restrict use of IoT device components (e.g., ports, functions, microphones, video)
	• Ability to logically or physically disable any local and network interfaces that are not necessary for the core functionality of the device
	• Ability to restrict updating actions to authorized entities
	• Ability to restrict access to the cybersecurity state indicator to authorized entities
	• Ability to restrict use of IoT device services
	• Ability to enforce the established local and remote access requirements
	• Ability to support wireless technologies needed by the organization (e.g., Microwave, Packet radio (UHF/VHF), Bluetooth, Manufacturer defined)
	• Ability to establish and configure IoT device settings for wireless technologies including wireless authentication protocols (e.g., EAP/TLS, PEAP)
		• AC-17 Remote Access
		• CM-7, Least Functionality
		• AC-3, Access Enforcement
		• AC-18, Wireless Access	

Sub-Capability	Key Abilities	Possible SP 800-53 Rev. 5 Controls Supported	Informative References
Software Update			
1. Update Application Support	• Ability to update the device's software through remote (e.g., network download) and/or local (e.g., removable media) means • If software updates are delivered and applied automatically: 　○ Ability to verify and authenticate any update before installing it 　○ Ability to enable or disable updating	• SI-2, Flaw Remediation	
Cybersecurity State Awareness			
1. Access to Event Information	• Ability to access information about the IoT device's cybersecurity state and other necessary data • Ability to preserve system state information	• SI-4, System Monitoring • AU-12, Audit Record Generation	
2. Event Identification & Monitoring	• Ability to identify organizationally-defined cybersecurity events (e.g., expected state change) that may occur on or involving the IoT device • Ability to monitor for organizationally-defined cybersecurity events (e.g., expected state change) that may occur on or involving the IoT device • Ability to support a list of events that are necessary for auditing purposes (to support organization's audit policy) • Ability to identify unique users interacting with the device (to allow for user session monitoring) • Ability to monitor communications traffic • Ability to detect remote activation attempts • Ability to detect remote activation of a collaborative computing device/component (e.g., microphone, camera) • Ability to define characteristics of unapproved content • Ability to scan files for unapproved content	• SI-4, System Monitoring • AU-2, Event Logging • IA-2, Identification and Authentication • SC-7, Boundary Protection • SC-15, Collaborative Computing Devices and Applications • CA-7, Continuous Monitoring	
3. Event Response	• Ability to generate alerts for specific events • Ability to respond to alerts with predefined responses • Ability to alert connected information systems of potential issues found during the auditing process • Ability to provide information to an external process that will issue auditing process alerts • Ability to notify users of activation of a collaborative computing device • Ability to respond following an auditing failure (either by the device or an external auditing process) • Ability to prevent download of unapproved content • Ability to delete unapproved content	• SI-4, System Monitoring • IR-4, Incident Handling • AU-6, Audit Record Review, Analysis, and Reporting • SC-15, Collaborative Computing Devices and Applications • AU-5, Response to Audit Logging Process Failures • RA-7 Risk Response	
4. Logging Capture & Trigger Support	• Ability to identify and capture organizationally-defined events using a persistent method • Ability to capture information from organizationally-defined cybersecurity events	• AU-2, Event Logging • AU-3, Content of Audit Records	

Sub-Capability	Key Abilities	Possible SP 800-53 Rev. 5 Controls Supported	Informative References
	(e.g., cybersecurity state, time) through organizationally-defined means (e.g., logs) • 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)		
5. Support of Required Data Logging	• 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 • Ability to log information pertaining to: o The type of event that occurred o The time that the event occurred o Where the event occurred o The source of the event o The outcome of the event o Identity of users/processes associated with the event • Ability to provide information as to why the device captured a particular event or set of events • Ability to capture organizationally-defined information to support examination of security incidents • Ability to record stored data access and usage	• AU-2, Event Logging • AU-3, Content of Audit Records	
6. Audit Log Storage & Retention	• Ability to comply with organizational policy for storing persistent audit logs up to a predefined size • Ability to comply with organizational policy for audit log retention period • Ability to delete audit logs in accordance with organizational policy	• AU-4, Audit Log Storage Capacity • AU-11, Audit Record Retention	
7. Support for Reliable Time	• Ability to use synchronization with a verified time source to determine the validity of a timestamp • Ability to record timestamps convertible to UTC or GMT to support a standardized representation of timing • Ability to log timing measurements outside a threshold value (e.g., enabling alerts if device's system time is not reliable)	• AU-8, Time Stamps	
8. Audit Support & Protection	• Ability to report on its cybersecurity state • Ability to support a self-audit generation process • 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.) • Ability to protect the audit information through the use of: o Encryption o Digitally signing audit files o Securely sending audit files to another device o Other protections created by the device manufacturer	• SI-4, System Monitoring • AU-6, Audit Record Review, Analysis, And Reporting • AU-9, Protection of Audit Information	

Sub-Capability	Key Abilities	Possible SP 800-53 Rev. 5 Controls Supported	Informative References
9. State Awareness Support	• Ability to differentiate between when a device will likely operate as expected from when it may be in a degraded cybersecurity state	• SI-5, Security Alerts, Advisories, and Directives	
Device Security			
1. Secure Execution	• Ability to execute code in confined virtual environments • Ability to separate IoT device processes into separate execution domains	• SC-39, Process Isolation	
2. Secure Communication	• Ability to enforce traffic flow policies • Ability to interface with DNS/DNSSEC	• SC-21, Secure Name/Address Resolution Service	
3. Secure Resource Usage	• Ability to manage memory address space assigned to processes • Ability to enforce access to memory space through the kernel • Ability to prevent a process from accessing memory space of another process • Ability to enforce configured disk quotas • Ability to utilize file compression technologies (e.g., to provide denial of service protection)	• SC-39, Process Isolation • SC-5, Denial of Service Protection	
4. Secure Device Operation	• Ability to define various operational states • Ability to restrict components/features of the IoT device (e.g., ports, functions, protocols, services) in accordance with organizationally-defined policies	• CP-10, System Recovery and Reconstitution • SC-24, Fail in Known State[11] • CM-7, Least Functionality • CP-12, Safe Mode	

336

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

342
343 **Table 2 - Non-technical Supporting Capabilities in the Federal Profile**

Sub-Capability	Key Actions	Primary SP 800-53 Rev. 5 Controls Supported	Informative References
Documentation			
1. Device Acquisition and	• Document all the IoT device security and privacy capabilities and limitations details.	• MA-1, Policy and Procedures	

---

[11] 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	• Document information necessary to inform the review and update of the IoT device systems, and the services' acquisition practices by IoT device customers. • 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. • 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. • Document the physical requirements, operational requirements, technical capabilities, and other related issues, required to sufficiently support all maintenance activities. • 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. • Document the physical and technical capabilities required to support the IoT device maintenance and diagnostic activities. • 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. • 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. • 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.	• MA-4, Nonlocal Maintenance • MA-5, Maintenance Personnel • PM-3, Information Security and Privacy Resources • SA-1, Policy and Procedures • SA-2, Allocation of Resources • SA-4, Acquisition Process • SI-4, System Monitoring	
2. Legal & Regulatory Compliance Support	• 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. • 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).	• SI-1, Policy and Procedures • PM-27, Privacy Reporting	

Sub-Capability	Key Actions	Primary SP 800-53 Rev. 5 Controls Supported	Informative References
3. Continuous Monitoring Support	• Document all the ways in which the IoT device can be monitored along with recommended associated tools to perform monitoring. • Document IoT device behavior and known indicators of attacks being launched on the IoT device. • Describe how to identify local, network and remote IoT device access attempts and connections. • Describe expected behavior of the normal operation of the IoT device.	• CA-7, Continuous Monitoring	
4. Documentation for Device Cybersecurity Capabilities	• Document information about capabilities within the IoT device that allow for unique identification of each IoT device. • 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. • Document information about how to use the IoT device capabilities to irreversibly remove all data from the device. • 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. • Document the manufacturer needs for access to the IoT device interfaces for support, updates, ongoing maintenance, etc. • Document the manufacturer requirements for data collection from the device. • Document the types of access to the IoT device the manufacturer will require on an ongoing and/or regular basis. • Document the role-based access capabilities built within the device, such as admin, general user, etc. • Document the IoT device's logical and remote interface access controls capabilities.	• AC-1, Policy and Procedures • CM-1, Policies and Procedures • CM-2, Baseline Configuration • IA-4, Identifier Management • PM-20, Dissemination of Privacy Program Information • PS-6, Access Agreements • SA-4, Acquisition Process • SI-4, System Monitoring • SI-12, Information Management and Retention	
5. Documentation for Post-Market Customer Activities	• Document how to configure the IoT devices, and related actions to take with the devices. • Document the process and detailed instructions for backing up data on the IoT device. • Provide documented instructions for implementing and using the unique IoT identifiers. • Document instructions for restricting interface connections that enable specific activities on the device. • 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. • Document how to configure the IoT device to technically support PIV implementation, accessibility and interfaces.	• AC-1, Policy and Procedures • AC-2, Account Management • AU-9, Protection of Audit Information • CM-1, Policies and Procedures • CM-2, Baseline Configuration • CP-9, System Backup • IA-1, Policy and Procedures • IA-2, Identification and Authentication	

Sub-Capability	Key Actions	Primary SP 800-53 Rev. 5 Controls Supported	Informative References
	• 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. • Document the indicators of unauthorized use of the IoT device. • Document the types of usage and environmental systems data that can be collected from the IoT device. • Document the IoT device security capabilities, security strength capabilities, and security assurance capabilities. • 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.	• IA-4, Identifier Management • PL-4, Rules of Behavior • PM-20, Dissemination of Privacy Program Information • PS-6, Access Agreements • SI-4, System Monitoring • SA-5, System Documentation	
Information and Query Reception			
1. Cybersecurity Feature Reports and Queries	• 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. • 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). • Document instructions for reporting/sending the manufacturer IoT device flaw reports. • 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. • Document procedures IoT customers need to follow to receive IoT device remediation reports from manufacturers. • 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.	• AC-1, Policy and Procedures • CM-1, Policies and Procedures • CM-2, Baseline Configuration • PM-20, Dissemination of Privacy Program Information • SI-2, Flaw Remediation • SI-3, Malicious Code Protection	
Information Dissemination			
1. Cybersecurity and Vulnerability Alerts	• Document the processes the manufacturer will follow to communicate their IoT device remediation efforts to their stakeholders (IoT device customers, users, etc.).	• CM-4, Impact Analyses	

Sub-Capability	Key Actions	Primary SP 800-53 Rev. 5 Controls Supported	Informative References
	• Document newly identified flaws and vulnerabilities for the associated IoT devices. • Document the anti-malware recommendations. If no anti-malware is needed for the IoT device, explain why. • Document the IoT device resource constraints for malicious code protection, and possible compensating controls that IoT device customers can use for such constraints. • Document a procedure to communicate information about cybersecurity incidents involving the IoT device to IoT device customers. • Document manufacturer's device flaw remediation efforts with stakeholders and IoT device customers.	• IR-1, Incident Response Policies and Procedures • MA-1, Policy and Procedures • SA-5, System Documentation • SI-2, Flaw Remediation • SI-3, Malicious Code Protection	
2. Software Update and Maintenance Notification	• 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. • Document instructions for IoT device customers to follow to review and update as necessary their IoT device systems and services practices, policies, and procedures. • 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.	• MA-2, Controlled Maintenance • SI-5, Security Alerts, Advisories, and Directives	
Education and Awareness			
1. Device Support Awareness	• 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). • 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. • Document and provide training materials to ensure IoT device customers understand the requirements for specified maintenance procedures. • 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. • Document and provide training materials to IoT device customers to ensure they understand the requirements for specified maintenance procedures.	• IR-2, Incident Response Training • MA-1, Policy and Procedures • MA-5, Maintenance Personnel • PL-1, Policy and Procedures	

14

Sub-Capability	Key Actions	Primary SP 800-53 Rev. 5 Controls Supported	Informative References
2. Device Cybersecurity Capability Awareness	• Document detailed instructions (e.g., using training videos, webinars, written directions) for implementing and using IoT device unique identifiers. • 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. • Document clear instructions and/or demonstrate (e.g., directly in person, in videos, in an online webinar) how to backup up the IoT device. • Document clear instructions, descriptions, and/or training for how to use the IoT device data removal capabilities and procedures. • Document instructions for how to establish and change role-based access settings. If role-based access capabilities are not available, document the limitation. • Document the types of security and privacy tests necessary for the IoT device and software before installation. • 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. • 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. • 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. • 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. • 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.	• AT-3, Role-based Training • CA-7, Continuous Monitoring • CM-1, Policies and Procedures • CM-2, Baseline Configuration • CM-4, Impact Analyses • CP-9, System Backup • IA-4, Identifier Management • PM-20, Dissemination of Privacy Program Information • SI-3, Malicious Code Protection • SI-12, Information Management and Retention	

Sub-Capability	Key Actions	Primary SP 800-53 Rev. 5 Controls Supported	Informative References
	• Document how to best implement and secure the IoT device and associated systems monitoring capabilities.		

344

345 **3   Conclusion**

346 The federal profile using the IoT core baseline and non-technical baseline is a helpful starting
347 point for both manufacturers and organizations to identify pertinent device cybersecurity
348 requirements (e.g., device cybersecurity capabilities and non-technical supporting capabilities)
349 needed to support system and organizational security goals. The capabilities included in the
350 profile are meant to represent those commonly needed by organizations to incorporate a device
351 into a system of low-impact (i.e., an information system that is determined to be of a low risk
352 impact based on a risk assessment). In some cases, the capabilities in the federal profile may be
353 sufficient for an organization to support their selected and tailored security controls and achieve
354 their security capabilities.

355 In other cases, the assumptions made in creating the federal profile and resulting device
356 cybersecurity capabilities and non-technical supporting capabilities may not be sufficient to meet
357 a specific organization's needs. Specific organizations may tailor controls and/or use common or
358 compensating controls that may render some capabilities in the profile not applicable or
359 insufficient to meet the specific organization's needs. Additionally, other organization goals
360 beyond cybersecurity (e.g., safety, privacy, reliability, resilience) that may be just as critical to
361 the organization's mission may further impact device cybersecurity requirements in ways the
362 federal profile cannot capture.

363 With these limitations in mind, organizations and manufacturers can use the federal profile as a
364 starting point to anticipate device cybersecurity and non-technical supporting capabilities needed
365 from and related to IoT devices. These limitations also mean that organizations and
366 manufacturers should work together wherever possible to identify device cybersecurity
367 requirements that apply to more specific organizations and use cases. Manufacturers and
368 customers should also be aware that all use cases cannot be predicted, especially for IoT devices
369 where one device could offer many uses. Manufacturers providing robust non-technical support,
370 including the kinds of documentation, actions, and other concepts discussed in this publication
371 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

373

374   **Appendix A—Acronyms**

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

376   ACD   Applied Cybersecurity Division

377   CSF   Cybersecurity Framework

378   DNS   Domain Name System

379   DNSSEC   Domain Name System Security Extensions

380   EAP   Extensible Authentication Protocol

381   FISMA   Federal Information System Modernization Act

382   GDPR   General Data Protection Regulation

383   GMT   Greenwich Mean Time

384   HIPAA   Health Insurance Portability and Accountability Act

385   ICS   Industrial Control Systems

386   IoT   Internet of Things

387   ITL   Information Technology Laboratory

388   IR   Internal Report

389   MAC   Media Access Control

390   NIST   National Institute of Standards and Technology

391   PEAP   Protected Extensible Authentication Protocol

392   RMF   Risk Management Framework

393   SP   Special Publication

394   TLS   Transport Layer Security

395   UHF   Ultra-High Frequency

396   UTC   Coordinated Universal Time

397   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 *core baseline*.

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.

400