

Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date November 29, 2021

Original Release Date December 15, 2020

Superseding Document

Status Final

Series/Number NIST Special Publication 800-213

Title IoT Device Cybersecurity Guidance for the Federal Government:
Establishing IoT Device Cybersecurity Requirements

Publication Date November 2021

DOI <https://doi.org/10.6028/NIST.SP.800-213>

CSRC URL <https://csrc.nist.gov/publications/detail/sp/800-213/final>

Additional Information SP 800-213A, *IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirements Catalog*,
<https://csrc.nist.gov/publications/detail/sp/800-213a/final>

2 **IoT Device Cybersecurity Guidance for**
3 **the Federal Government:**

4 *Establishing IoT Device Cybersecurity Requirements*

5
6 Michael Fagan
7 Jeffrey Marron
8 Kevin G. Brady, Jr.
9 Barbara B. Cuthill
10 Katerina N. Megas
11 Rebecca Herold

12
13
14
15 This publication is available free of charge from:
16 <https://doi.org/10.6028/NIST.SP.800-213-draft>

20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42

Draft NIST Special Publication 800-213

IoT Device Cybersecurity Guidance for the Federal Government:

Establishing IoT Device Cybersecurity Requirements

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

Rebecca Herold
*The Privacy Professor
Des Moines, IA*

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

December 2020



43
44
45
46
47
48
49
50

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

51

Authority

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

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

65 National Institute of Standards and Technology Special Publication 800-213
66 Natl. Inst. Stand. Technol. Spec. Publ. 800-213, 30 pages (December 2020)
67 CODEN: NSPUE2

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

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

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

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

83

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

85 National Institute of Standards and Technology
86 Attn: Applied Cybersecurity Division, Information Technology Laboratory
87 100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
88 Email: iotsecurity@nist.gov

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

90 **Reports on Computer Systems Technology**

91 The Information Technology Laboratory (ITL) at the National Institute of Standards and
92 Technology (NIST) promotes the U.S. economy and public welfare by providing technical
93 leadership for the Nation’s measurement and standards infrastructure. ITL develops tests, test
94 methods, reference data, proof of concept implementations, and technical analyses to advance the
95 development and productive use of information technology. ITL’s responsibilities include the
96 development of management, administrative, technical, and physical standards and guidelines for
97 the cost-effective security and privacy of other than national security-related information in federal
98 information systems. The Special Publication 800-series reports on ITL’s research, guidelines, and
99 outreach efforts in information system security, and its collaborative activities with industry,
100 government, and academic organizations.

101 **Abstract**

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

111 **Keywords**

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

114

Supplemental Content

115 The NIST Cybersecurity for IoT Team has undertaken an effort that aims to help manufacturers
116 and federal government agencies better understand what kinds of device cybersecurity
117 capabilities and supporting non-technical capabilities may be needed from or around IoT devices
118 used by federal government agencies. To that end, NIST has developed a catalog
119 (<https://pages.nist.gov/IoT-Device-Cybersecurity-Requirement-Catalogs/>) of IoT device
120 cybersecurity capabilities and supporting non-technical capabilities for manufacturers and IoT
121 device customers. This catalog identifies technical and non-technical capabilities that may be
122 necessary for supporting NIST SP 800-53 controls implemented in federal information systems.
123 Just as not every Federal IT system uses every control, not every capability in the catalog is
124 needed in every IoT device. Ultimately, the goal is to enable federal agencies to securely
125 incorporate IoT devices into their information systems and meet their security requirements.

126

Acknowledgments

127 The authors wish to thank all contributors to this publication, including the participants in
128 workshops and other interactive sessions; the individuals and organizations from the public and
129 private sectors, including manufacturers from various sectors as well as several manufacturer
130 trade organizations, who provided feedback on the preliminary public content and colleagues at
131 NIST who offered invaluable inputs and feedback. Special thanks to Cybersecurity for IoT team
132 members Brad Hoehn and Dave Lemire and the NIST FISMA Implementation Project team for
133 their extensive help in copy editing.

134

Audience

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

138

139

Call for Patent Claims

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

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

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

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

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

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

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

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

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

165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193

Table of Contents

1 Introduction 1

 1.1 Purpose and Applicability..... 1

 1.2 Target Audience..... 2

 1.3 Relationship to Other Publications 2

 1.4 Document Conventions..... 3

 1.5 Publication Organization 3

2 Background Considerations 4

 2.1 Systems and Elements 4

 2.2 How IoT Devices Support Security 5

 2.3 How IoT Devices May Create Security Challenges..... 8

3 Identifying Device Cybersecurity Requirements for IoT Devices 10

 3.1 Important IoT Device Cybersecurity Considerations 10

 3.2 Sources of Device Cybersecurity Requirements..... 13

 3.3 Use Context and Other Organization-Specific Information 15

References 18

List of Appendices

Appendix A— Acronyms 221

Appendix B— Glossary 222

List of Figures

Figure 1 - Visualization of the System and Environment..... 4

Figure 2 - Information Security Requirements Integration to the Element Level 6

Figure 3 - Role of Device Cybersecurity and Non-Technical Supporting Capabilities in
Satisfying Security Capabilities and Requirements 7

Figure 4 - Information Sources to Identify Device Cybersecurity Requirements 10

194 **1 Introduction**

195 As Internet of Things (IoT) technology evolves, it is inevitable that most federal agencies will
196 integrate this equipment into federal information systems¹. IoT² technology creates many
197 opportunities for federal agencies in support of mission objectives. IoT technology may also
198 present cybersecurity challenges if proper considerations are not made during the acquisition and
199 integration of an IoT device.

200 Existing NIST risk management guidance helps federal agencies satisfy their security
201 requirements³ from the information system level up through the organizational⁴ level. However,
202 the increasing scale, heterogeneity, and pace of IoT deployment motivates a focus on security
203 requirement support below the information system level, at the system element level⁵. IoT
204 devices used by federal agencies will frequently be integrated as system elements, and this
205 integration will often happen well after the information system has been initially deployed. As an
206 example, an agency may purchase voice-activated printers and integrate them into the existing
207 enterprise network. Agencies must also grapple with the challenge that many IoT devices lack
208 features and functions that are common in conventional information technology (IT) equipment.

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

213 **1.1 Purpose and Applicability**

214 This publication is intended to help federal agencies incorporate IoT devices into an existing
215 information system as system elements. IoT devices in-scope for this publication have at least
216 one transducer (sensor or actuator) for interacting directly with the physical world and at least
217 one network interface (e.g., Ethernet, Wi-Fi, Bluetooth, Long-term Evolution (LTE), Zigbee,

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

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

³ As identified in SP 800-53 Rev. 5, *security requirements* are “applicable laws, executive orders, directives, regulations, policies, standards, procedures, or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted.”

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

⁵ A *system element* is discrete part of a system such as a device, equipment, or application that is connected to other system elements and works with them to achieve the system’s goals. IoT devices will commonly be system elements relative to the federal information system they are connected to.

218 Ultra-Wideband (UWB)) for interfacing with the digital world. The IoT devices in-scope for this
219 publication can function on their own, although they may be dependent on specific other devices
220 (e.g., an IoT hub) or systems (e.g., a cloud) for some functionality⁶. While this publication
221 might be helpful for IoT products that fall outside this scope or for other situations (e.g., when
222 IoT devices are being integrated as system elements from the conception of an information
223 system), other NIST publications, such as the Risk Management Framework (RMF) suite of
224 security standards and guidance, address those situations more directly.

225 **1.2 Target Audience**

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

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

239 **1.3 Relationship to Other Publications**

240 This publication uses concepts from the NIST Risk Management Framework, specifically
241 publications such as NIST SPs 800-18 [2], 800-30 [3], 800-37 [4], 800-39 [5], 800-53 [6], 800-
242 60 [7], 800-82[8], and 800-160 v1 [9] and v2 [10] as well as the NIST Cybersecurity Framework
243 [11]. It also follows from the foundational cybersecurity for IoT work from NIST documented in
244 NISTIR 8228 [12]and the NISTIR 8259 series [13, 14, 15, 16, 17]. Details on the relationship to
245 these other publications is in Section 2.

246 This publication uses both the terms “security” and “cybersecurity.” For most purposes, these
247 terms are interchangeable and relate to protecting confidentiality, integrity, and availability of
248 data, but as convention, security is used when discussing the protection of these for the system
249 while cybersecurity is used when discussing how elements might support security or protect
250 security themselves. This mixed terminology is motivated by common use of the term security in
251 the RMF, but the term cybersecurity is used for the same concepts in IoT to avoid confusion with
252 physical security/safety requirements.

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

253 **1.4 Document Conventions**

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

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

- 257 a. Where the term “shall” is used, the statement is to be interpreted as a requirement.
258 b. Where the term “should” is used, the statement is to be interpreted as a
259 *recommendation*.

260 **1.5 Publication Organization**

261 The rest of this publication is organized as follows:

- 262 ● Section 2 provides background considerations and connects the challenges presented by
263 IoT devices with risk management practices discussed in NIST publications.
264 ● Section 3 details how the background considerations in Section 2 can be used with
265 existing sources to identify device cybersecurity requirements.

2 Background Considerations

This section presents background information about IoT devices that agencies should consider in their device acquisition processes. This publication draws from other NIST guidance, namely the Risk Management Framework (RMF) [4] and the Cybersecurity Framework (CSF) [11]. Since IoT devices will often be integrated into existing federal information systems, this publication will provide guidance for agencies in the context of the RMF.

2.1 Systems and Elements

As discussed in Section 1, federal cybersecurity risk management processes generally consider the security of organizations and systems; but systems are made up of elements. Increasingly, IoT devices may become elements of federal information systems. The relationship between systems and elements is a foundational concept in this publication. To understand more about this relationship between systems and elements, readers should refer to NIST Special Publication 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [4]. Some of the key concepts, particularly those covered in section 2.4 of SP 800-37, will be highlighted here. Figure 1 shows these concepts visually, adapted from a figure in SP 800-37, Revision 2.

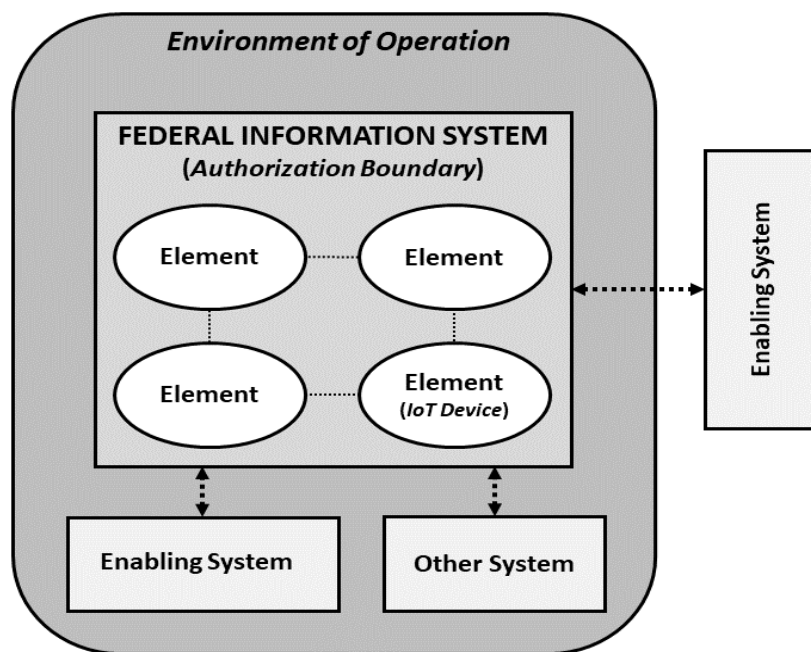


Figure 1 - Visualization of the System and Environment

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

285 The information system can also be supported by other enabling systems, which will fall outside
286 the authorization boundary. Information systems can also interact with other systems, which
287 might be beneficiaries of capabilities offered by the information system. The federal information
288 system—as well as some enabling and other systems—will fall within the environment of
289 operation, which is the physical environment in which these systems reside and operate.

290 As explained in SP 800-37, federal agencies define and determine the parts of the environment of
291 operation that are within the authorization boundary of each information system. As shown in
292 Figure 1, the environment of operation can contain multiple authorization boundaries, including
293 other systems and enabling systems. Elements, including IoT devices, may interact and
294 communicate across multiple systems/authorization boundaries. However, for accountability
295 and risk management purposes, each IoT device is only included within one authorization
296 boundary, in general. Additional enabling systems will fall outside of the environment of
297 operation (e.g., a system hosted by another agency or service provider). This concept of systems
298 and elements can help clarify the ways IoT devices might be used by federal agencies and the
299 subsequent identification of device cybersecurity requirements.

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

306 Other IoT devices acquired by federal agencies will be best characterized as system elements that
307 fall within the authorization boundary of an existing information system. This is depicted in
308 Figure 1 by the element in the bottom right corner of the authorization boundary. Since the
309 device will be integrated as a system element, agencies may have significantly more expectations
310 about how this IoT device must support the security controls of the information system and/or
311 organization. If the IoT device lacks technical and non-technical capabilities (discussed further in
312 Section 2.2) to support the information system's security controls, challenges can arise for the
313 agency. In this situation, the agency may need to implement compensating controls (e.g.,
314 creating a segmented network for IoT) or costly reimplementations of existing controls. If risk(s)
315 introduced by the IoT device cannot be mitigated, the agency may have to accept these new risks
316 or decide to not incorporate the IoT device into the information system.

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

323 **2.2 How IoT Devices Support Security**

324 The relationship of an IoT device to an information system provides the context to understand
 325 how an IoT device supports both information system and organizational objectives. NIST SP
 326 800-39, *Managing Information Security Risk: Organization, Mission, and Information System*
 327 *View* [5], discusses how higher-level mission and organizational objectives inform the
 328 architecture and control structure around information systems. In this publication, we extend the
 329 discussion from SP 800-39, highlighting the connection between systems and elements as
 330 discussed in SP 800-37 and Section 2.1 above. Figure 2 shows the connection between the
 331 concepts discussed in SP 800-39 and system elements.

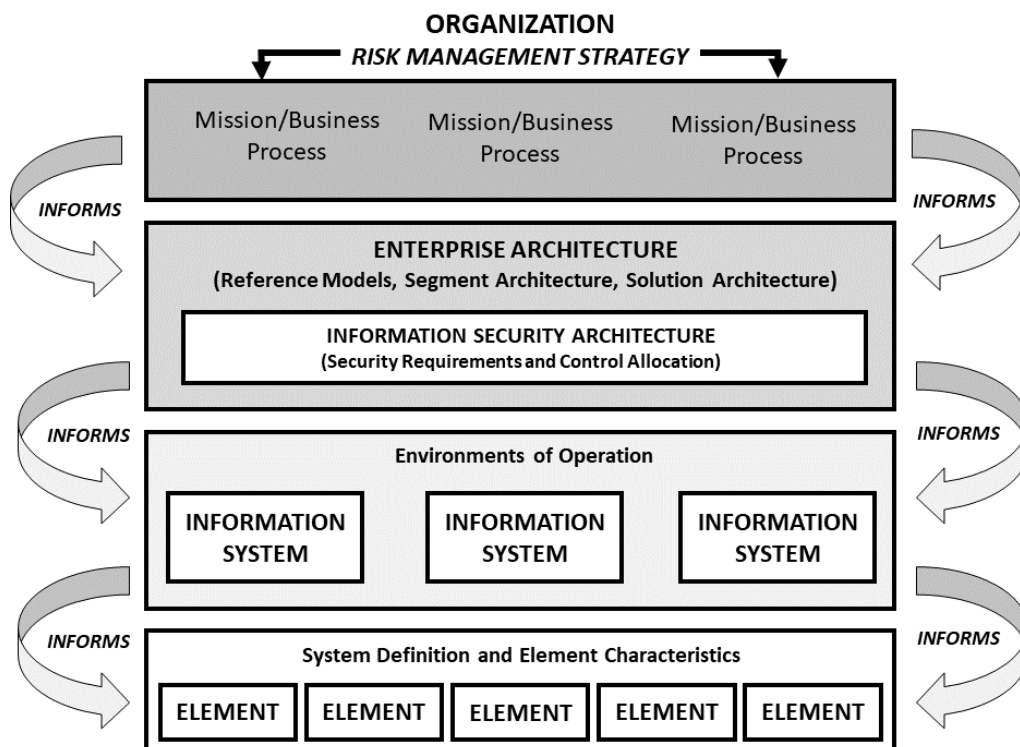


Figure 2 - Information Security Requirements Integration to the Element Level

332 SP 800-39 describes how the organization’s risk management strategy informs the enterprise
 333 architecture, including the information security architecture. Key to the information security
 334 architecture is the identification of security requirements and the selection and allocation of
 335 security controls. The information security architecture informs the information systems within
 336 the environments of operation, particularly through the application of security controls. This
 337 publication focuses on IoT devices as system elements that must both support and be informed
 338 by the information system and its security controls.

339 The primary way that IoT devices support security controls is via technical means, which are
 340 called *device cybersecurity capabilities*. The NISTIR 8259 series discusses the concept of device
 341 cybersecurity capabilities extensively from the manufacturer’s perspective—that is, for
 342 manufacturers to understand the capabilities that customers need in IoT devices. But the
 343 information in the NISTIR 8259 series could also be helpful for federal agencies. In particular,

344 NISTIR 8259D, *Profile of the IoT Core Baseline for the Federal Government* [17], focuses on
 345 the federal government as a sector of IoT device customers and identifies foundational device
 346 cybersecurity capabilities needed in IoT devices acquired by the federal government. NISTIR
 347 8259D also identifies *non-technical supporting capabilities*, which are actions that
 348 manufacturers or third parties take in support of the initial and on-going security of IoT devices.

349 **Example Device Cybersecurity and Non-Technical Supporting Capabilities**

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

355 Both device cybersecurity capabilities and non-technical supporting capabilities are vital to
 356 federal agencies' ability to implement controls that the agency has allocated for their federal
 357 information systems. Figure 3 illustrates how device cybersecurity capabilities and non-technical
 358 supporting capabilities (grouped together as 'Device Cybersecurity Requirements') support
 359 system/organizational security capabilities, which in turn satisfy organizational security
 360 requirements.

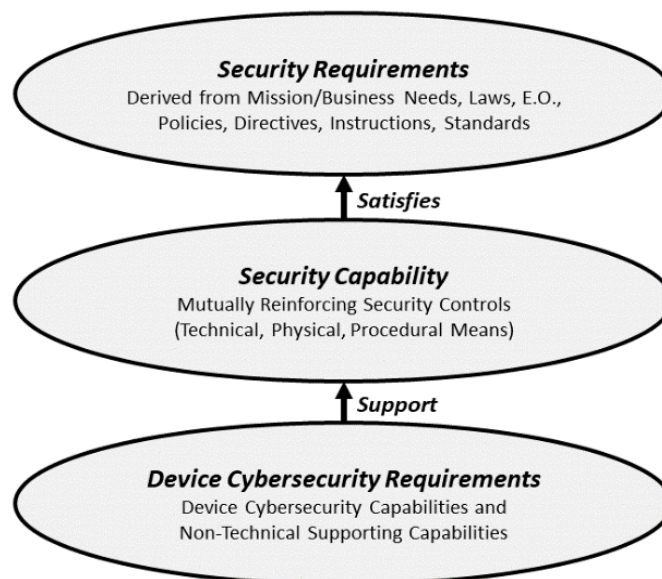


Figure 3 - Role of Device Cybersecurity and Non-Technical Supporting Capabilities in Satisfying Security Capabilities and Requirements

361 Allocation and application of security controls to information systems is a key step of risk
 362 management. Controls used by the federal government generally are selected from the NIST SP
 363 800-53, Revision 5 *Security and Privacy Controls for Information Systems and Organizations*
 364 [6]. These controls are technology agnostic and can apply to IoT devices incorporated into
 365 federal information systems as system elements.

IoT Devices in the Context of the Risk Management Framework

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

The guidance in this publication focuses on establishing device cybersecurity requirements to support security controls. This publication does not provide details on how IoT devices may impact an information system's risk assessment or reallocation of controls that may be necessary. Readers are encouraged to reference SP 800-30, *Guide for Conducting Risk Assessments* and other publications in the RMF suite of publications for guidance on assessing risk due to the inclusion of an IoT device into an information system.

2.3 How IoT Devices May Create Security Challenges

Integrating an IoT device into an information system can present a number of challenges for federal agencies. Federal agencies should strive to understand these challenges before an IoT device is integrated into an information system. For example, due to a number of market and technological factors, IoT devices often lack security functionality commonly present in conventional IT equipment (e.g., laptops). A lack of security functionality in an IoT device could introduce unacceptable levels of risk to the information system. NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* [12] details some of these challenges that IoT devices can create for federal agencies. The challenges described in NISTIR 8228 represent generic, high-level use cases. For specific agencies or particular IoT devices, the challenges faced could diverge from those explored in NISTIR 8228. Agencies are encouraged to apply the concepts in NISTIR 8228 to identify challenges applicable to their use cases.

Overview of NISTIR 8228 Concepts

NISTIR 8228 explores a number of challenges, grouped around conventional risk mitigation areas such as asset management, data protection, incident detection, and vulnerability management. The publication further groups these areas into goals of protecting device security, data security, and/or individual privacy. Challenges can arise that hinder risk mitigations in various areas or could impact some or all of the goals. For example, to mitigate risks related to vulnerability management, software updates may need to be performed. However, not all IoT devices allow for software updates (Challenges 8, 10, and 11). Even mitigations as simple as hiding passwords might not be achievable on IoT devices (Challenge 17).

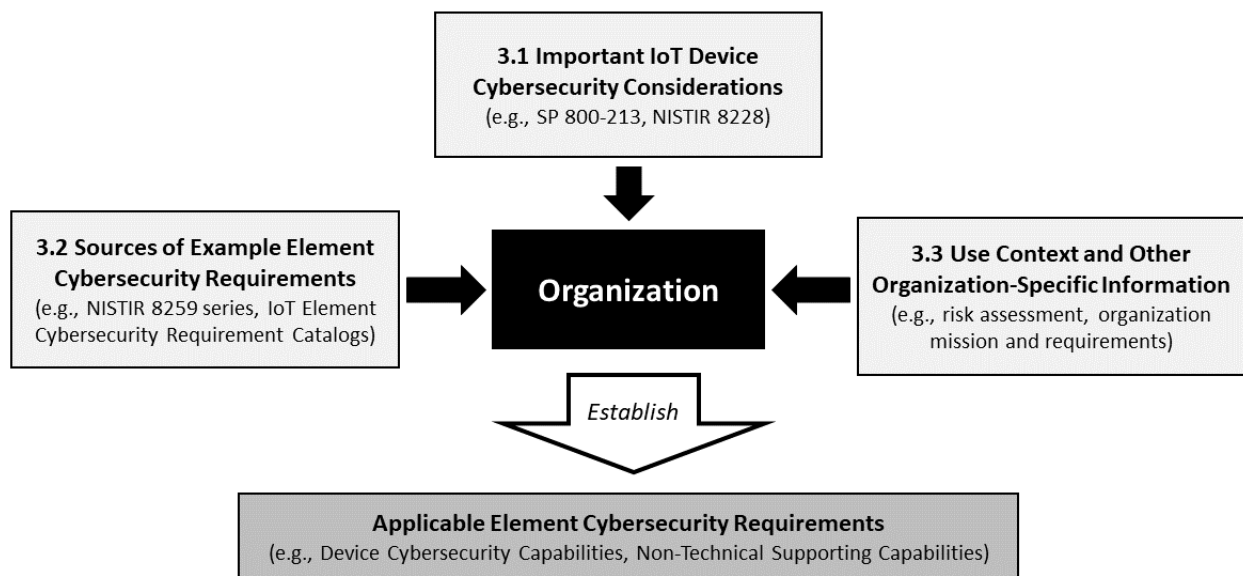
Federal agencies should not underestimate the challenges of integrating an IoT device into an information system. NIST SP 800-160, Volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* [9]

403 demonstrates how an integrated process is best for engineering trustworthy systems. SP 800-160
404 presents concepts reflected in other NIST SPs from a system engineering perspective, giving a
405 detailed look at how trustworthy systems can be engineered. The approach outlined in SP 800-
406 160 considers acquisition early in system design and integration later, which are important
407 concepts in building a trustworthy system. Federal agencies are encouraged to apply concepts
408 from SP 800-160 when integrating IoT devices into information systems to ensure the
409 trustworthiness of the information system.

410 Federal information systems will frequently be engineered at one point in time, but then
411 modified as system elements are removed or other elements added. When IoT devices are added
412 as system elements, federal agencies should consider how the integration of the IoT device could
413 impact system and organizational security requirements. However, integrating an IoT device
414 into an information system can also be aided by taking a device-centric perspective. Through a
415 device-centric perspective, a federal agency can identify and articulate the device cybersecurity
416 requirements (i.e., the set of device cybersecurity capabilities and non-technical supporting
417 capabilities) required from IoT devices and manufacturers/third parties to support security
418 capabilities and satisfy security requirements. Federal agencies should be aware that even if the
419 articulated device cybersecurity requirements are provided by a device and manufacturer/third
420 party, the integration of the IoT device into an information system can still introduce risk.

3 Identifying Device Cybersecurity Requirements for IoT Devices

This section provides guidance to federal agencies in determining the applicable device cybersecurity requirements (i.e., the set of device cybersecurity capabilities and non-technical supporting capabilities) for an IoT device. Figure 4 illustrates the information sources that agencies can use to help identify device cybersecurity requirements. Each type of source is explored in more detail in this section.



427

428

Figure 4 - Information Sources to Identify Device Cybersecurity Requirements

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

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

3.1 Important IoT Device Cybersecurity Considerations

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

447 agencies may seek to leverage IoT technology in the delivery of services to citizens.

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

453 **1. What is the benefit of the IoT device and how will it be utilized?** Agencies can help
454 ensure that device cybersecurity requirements receive proper consideration by
455 establishing an explicit benefit for integrating the IoT device and understanding how the
456 IoT device will be used. For example, is the IoT device replacing equipment that did not
457 connect to the information system? In such a case, agencies should consider the benefit of
458 the system connection compared to the potential risks.

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

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

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

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

473 **3. In what technologies will the data be stored?** Many IoT devices maintain connections
474 to cloud services and mobile/web applications that are central to the device's
475 functionality. IoT devices can also connect to additional external services, which may be
476 provided and hosted by a number of third parties. Agencies should consider where the
477 IoT device might store data—in the device, the manufacturer's network, a manufacturer-
478 contracted entity's network (e.g., cloud), etc.

479 **4. In what geographic areas will the data be shared and/or stored?** The architecture that
480 supports IoT devices is increasingly global. Federal agencies should consider where data
481 from prospective IoT devices will be transmitted and stored to ensure applicable security
482 requirements are met. An IoT device may connect to and transmit data to systems in
483 many diverse areas, including other cities, states, and countries. These connections may
484 change over time due to the dynamic nature of IoT systems.

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

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

- 493 1. **Might the device interfere with other aspects of operations or system functionality?**
494 Unlike conventional IT equipment, IoT devices are more likely to interact with the
495 physical world through sensing and/or actuating. This interaction increases the possibility
496 that a compromised IoT device could affect operations and the environment (e.g., alarms,
497 thermostats, environmental controls, heating elements) as well as the security posture of
498 the information system. For example:
- 499 a. *Could the IoT device introduce privacy or safety risks for people?* IoT devices
500 could collect and share sensitive data about people, including audio and video
501 data. An IoT device can also interact with the physical world (e.g., IoT vehicle) or
502 might be intended to protect human safety (e.g., an IoT smoke alarm), potentially
503 posing safety risks. Considering if an IoT device may introduce privacy or safety
504 risks is critical to planning for risk mitigation.
 - 505 b. *Could the IoT device interfere with system reliability or resiliency?* The diversity
506 of IoT device use cases also creates the possibility that the IoT device's expected
507 operational environment may vary from where it is actually deployed. In such an
508 instance, the IoT device might negatively interact with other system elements or
509 operational systems in federal agencies if not properly planned for. For example,
510 an IoT device may go offline to apply a software update. This behavior is
511 acceptable in many circumstances but may hurt system reliability if the offline
512 device hurts operations in other parts of the system. Likewise, IoT devices may
513 not be as digitally and physically resilient as their IT or OT counterparts since IoT
514 devices must sometimes attempt to deliver both IT and OT functionality.
- 515 2. **Would the IoT device introduce unacceptable risks to the agency or result in non-**
516 **compliance with cybersecurity requirements?** Organizations should also consider how
517 they will secure the IoT device and mitigate any associated risks in accordance with their
518 cybersecurity requirements. IoT devices can alter the level of impact (i.e., low, moderate,
519 high) that has been determined for a system, which could, in turn, require additional
520 controls. Some IoT devices might be unable to support the organization's current
521 cybersecurity strategies due to their design, requiring agencies to implement
522 compensating controls for the IoT device (e.g., network segmentation).
- 523 3. **Is the IoT device known to have had published security and/or privacy**
524 **vulnerabilities?** Like all connected products, IoT devices attract attention from security
525 professionals and researchers who identify security and/or privacy concerns.
526 Manufacturers also commonly publish similar information concerning their devices.
527 Federal agencies should look to these disclosures to inform themselves of known
528 vulnerabilities. If the manufacturer cannot mitigate the vulnerabilities, agencies would
529 have to identify and address risks introduced by the IoT device.

530 As discussed extensively in NISTIR 8228, IoT devices can have significantly different feature
531 sets compared to conventional IT devices. These differences in device capabilities and support
532 for security controls can create challenges for federal agencies if not adequately planned for.
533 Federal agencies should refer to NISTIR 8228 and consider if the IoT device will create any
534 security and privacy challenges for the information system and organization. Consider:

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

- 537 1. *Does the IoT device lack key device cybersecurity requirements?* Key device
538 cybersecurity requirements are those the agency has determined that the IoT
539 device must possess in order for the device to be integrated in the federal
540 information system. Lack of key device cybersecurity requirements means that
541 the IoT device cannot support existing information system controls and/or
542 subsequently introduces unacceptable levels of risk to the information system.
- 543 2. *Will the implementation or maturity of device cybersecurity capabilities and/or*
544 *non-technical supporting capabilities fail to satisfy the agency's key device*
545 *cybersecurity requirements?* Some IoT devices may completely lack key device
546 cybersecurity requirements, making the IoT device unusable by the federal
547 agency. Other IoT devices may provide device cybersecurity requirements but not
548 in the manner expected by the federal agency. For example, an IoT device may
549 have a unique device identifier, but it may not be in a format the federal agency
550 uses with other equipment. The agency will need to plan for how this identifier
551 will be incorporated into its asset management processes. When an IoT device's
552 cybersecurity capabilities lack maturity, the task of securing the device may be
553 much more difficult. For example, an IoT device may encrypt data, but use a
554 deprecated encryption module due to device resource constraints. In this case,
555 agencies may need to apply significant compensating controls.

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

558 **3.2 Sources of Device Cybersecurity Requirements**

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

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

570 NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers* [13], directs
571 manufacturers to support the cybersecurity needs and goals of expected IoT device customers in
572 the device’s expected use case. The manufacturer’s primary role is to ensure minimal
573 securability, providing the minimum necessary device cybersecurity capabilities and non-
574 technical supporting capabilities to meet customer needs and goals. NISTIR 8259A, *IoT Device*
575 *Cybersecurity Capability Core Baseline* [14] specifies the high-level device technical
576 cybersecurity capabilities that generally achieve minimal securability for most customers. The
577 IoT core baseline, as the IoT device cybersecurity capability core baseline from NISTIR 8259A
578 is called, is meant to apply to all IoT use cases and customers, meaning it is phrased at a high
579 level to meet many different needs. NISTIR 8259B, *IoT Non-Technical Supporting Capability*
580 *Core Baseline* [15] presents a set of non-technical supporting capabilities—the IoT non-technical
581 supporting capability core baseline—generally needed from manufacturers or other third parties
582 to support common cybersecurity controls. Like 8259A, the non-technical capabilities in 8259B
583 are phrased at a high level to be broadly applicable to various use cases and customers.

584 The IoT core baselines presented in NISTIR 8259A and 8259B can be profiled for a specific
585 customer, sector, or use case. The process of profiling tailors and/or extends the IoT core
586 baselines and can be performed at any level of specificity, even to an individual customer (e.g.,
587 federal agency). NISTIR 8259C, *Creating a Profile Using the IoT Core Baseline and Non-*
588 *technical Baseline* [16], discusses this process of profiling the IoT core baselines to identify IoT
589 device requirements that best meet the customer’s cybersecurity needs and goals.

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

591 Readers may be familiar with the low-, moderate-, and high-impact security control baselines in
592 the NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*. The IoT
593 core baselines are distinct from the SPP 800-53B security control baselines and shall be
594 considered separately. The device cybersecurity capabilities and non-technical supporting
595 capabilities presented in the IoT core baselines enable IoT devices to *support* the controls in a SP
596 800-53B control baseline.

597 NISTIR 8259D presents a profile of the IoT core baselines that is guided by the needs and goals
598 of federal agencies. The federal profile in NISTIR 8259D uses the SP 800-53 controls catalog as
599 an input source of federal government cybersecurity needs and goals. Whereas the controls in SP
600 800-53 generally focus on the information system and organization, the capabilities in the federal
601 profile articulate the device cybersecurity capabilities and non-technical supporting capabilities
602 needed to support the controls. The federal profile considers the IoT device as an information
603 system element in which SP 800-53 security controls have already been identified and allocated.

604 Since the federal profile in NISTIR 8259D targets minimal securability for all federal
605 government use cases, it focuses on device capabilities that support the low-impact baseline set
606 of SP 800-53 controls. This focus is based on the assumption that the low-impact baseline set of
607 controls—with minimal tailoring and application of compensating controls—will be used for
608 many federal information systems. The federal profile in NISTIR 8259D is therefore
609 recommended as a starting point for federal agencies to use when identifying IoT device

610 cybersecurity requirements ⁷. The use of the low-impact baseline will not be appropriate for all
611 agencies and use cases, particularly if an IoT device is integrated into a moderate- or high-impact
612 information system. The device cybersecurity requirements in the federal profile may not
613 adequately support the security controls in moderate- and high-impact information systems.

614 In addition to the IoT core baselines and federal profile, federal agencies may also leverage the
615 IoT Device Cybersecurity Requirement Catalogs [[https://pages.nist.gov/IoT-Device-
616 Cybersecurity-Requirement-Catalogs/](https://pages.nist.gov/IoT-Device-Cybersecurity-Requirement-Catalogs/)]. These two catalogs contain additional device
617 cybersecurity requirements organized by technical (i.e., device cybersecurity capabilities) and
618 non-technical (i.e., non-technical supporting capabilities). The device cybersecurity requirements
619 in the catalogs are derived from security controls in SP 800-53 and therefore may be helpful in
620 supporting security controls in moderate and high impact information systems. The NIST Pages
621 Catalogs can be a valuable resource for federal agencies when identifying applicable IoT device
622 cybersecurity requirements.

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

631 **3.3 Use Context and Other Organization-Specific Information**

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

638 Since IoT device cybersecurity requirements are in support of security controls allocated to
639 information systems, federal agencies can identify the device cybersecurity requirements needed
640 to support the security controls allocated to the information system(s) to which the IoT device
641 will be connected. Information security and systems administration personnel should collaborate
642 to identify security controls that require support from system elements (e.g., IoT devices).

643 Federal agencies should remember that the incorporation of an IoT device can alter the
644 information system's risk assessment. Any change in the risk assessment may require the
645 allocation of additional security controls or the introduction of compensating controls to reduce
646 risk to acceptable levels. Section 3.1 provides a starting point for considerations about IoT

⁷ Manufacturers may choose to incorporate the device cybersecurity requirements from the federal profile in their IoT devices, especially for IoT devices where federal agencies are an expected customer

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

656 **Example of Device Cybersecurity Requirements Supporting Security Controls**

657 An agency might want to acquire an IoT device such as a *smart speaker* to use in the office
658 environment. The smart speaker will need to connect to the federal information system (e.g.,
659 internal network) so that agency management can remotely (but within the environment of
660 operation) access and play audio over the speaker. These remote connections will require proper
661 authentication and authorization. To support the authentication and authorization controls, the
662 smart speaker may require device cybersecurity capabilities such as the ability to deny remote
663 connections; the ability to authenticate and/or authorize entities attempting to make remote
664 connections; and the ability to terminate connections within organizational policy. Other device
665 cybersecurity capabilities may apply, but these are presented as example capabilities.
666 Additionally, the allocated security controls may require the federal agency to configure the
667 smart speaker to authenticate and authorize users within organizational policy, which could
668 require non-technical supporting capabilities from manufacturers. These non-technical
669 supporting capabilities could include obtaining documentation from the manufacturer about how
670 the IoT device can be configured to support organizational authentication and authorization
671 policy.

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

679 **Organization-specific Considerations Impact Device Cybersecurity Requirements**

680 When selecting IoT device cybersecurity requirements, agencies also need to consider how
681 organization-specific policies, procedures, or environment may affect device cybersecurity
682 requirements. In the previous call-out box, an example was presented of a smart speaker that
683 requires proper authentication and authorization before allowing connections. Does the agency
684 require Personal Identity Verification (PIV) card-based authentication or does it allow password-
685 based authentication in limited circumstances? These agency policies will influence IoT device
686 cybersecurity requirements. Does the agency purchase products from particular manufacturers

687 or 3rd parties? The IoT devices available to the agency through those parties may limit the
688 device cybersecurity capabilities and non-technical supporting capabilities available. Are there
689 any environmental considerations (e.g., temperature, humidity, etc.) in the environment of
690 operation? If so, device requirements may need to account for these environmental
691 considerations. These organization-specific considerations may impact not only the device
692 cybersecurity requirements, but also the design of the device. In the examples above, perhaps
693 the IoT device needs to provide support for derived PIV credentials, or the IoT device may need
694 to have a durable housing to withstand excessive heat while still providing functionality.
695 Agencies will need to carefully account for these organizational considerations that may impact
696 device requirements.

697 **References**

- [1] Petersen R, Santos D, Wetzel K, Smith M, Witte G (2020) Workforce Framework for Cybersecurity (NICE Framework). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181 Rev. 1 <https://doi.org/10.6028/NIST.SP.800-181r1>
- [2] Swanson M, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18 <https://doi.org/10.6028/NIST.SP.800-18r1>
- [3] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-30r1>
- [4] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. <https://doi.org/10.6028/NIST.SP.800-37r2>
- [5] Joint Task Force Transformation Initiative (2011) Manage Information Security Risk. (National Institute of Standards and Technology, Gaithersburg, MD) NIST Special Publication (SP) 800-39 <https://doi.org/10.6028/NIST.SP.800-39>
- [6] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. <https://doi.org/10.6028/NIST.SP.800-53r5>
- [7] Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 1, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-60v1r1>
- [8] Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 2. <https://doi.org/10.6028/NIST.SP.800-82r2>
- [9] Ross RS, Oren JC, McEvelley M (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018. <https://doi.org/10.6028/NIST.SP.800-160v1>
- [10] Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R (2019) Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 2. <https://doi.org/10.6028/NIST.SP.800-160v2>

- [11] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). <https://doi.org/10.6028/NIST.CSWP.04162018>
- [12] Boeckl K, Fagan M, Fisher W, Lefkovitz N, Megas K, Nadeau E, Piccarreta B, O'Rourke DG, Scarfone K (2018) Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8228 <https://doi.org/10.6028/NIST.IR.8228>
- [13] Fagan M, Megas KN, Scarfone K, Smith M (2020) Foundational Cybersecurity Activities for IoT Device Manufacturers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259. <https://doi.org/10.6028/NIST.IR.8259>
- [14] Fagan M, Megas KN, Scarfone K, Smith M (2020) IoT Device Cybersecurity Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259A. <https://doi.org/10.6028/NIST.IR.8259A>
- [15] Fagan M, Marron J, Brady KG, Jr, Cuthill BB, Megas KN, Herold R (2020) IoT Non-Technical Supporting Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Interagency or Internal Report (IR) 8259B. <https://doi.org/10.6028/NIST.IR.8259B-draft>
- [16] Fagan M, Marron, J, Brady KG, Jr, Cuthill BB, Megas KN, Herold R (2020) Creating a Profile Using the IoT Core Baseline and non-technical baseline. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Interagency or Internal Report (IR) 8259C. <https://doi.org/10.6028/NIST.IR.8259C-draft>
- [17] Fagan M, Marron, J, Brady KG, Jr, Cuthill BB, Megas KN, Herold R (2020) Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259D. <https://doi.org/10.6028/NIST.IR.8259D-draft>
- [18] Cyber-Physical Systems Public Working Group (2017) Framework for Cyber-Physical Systems: Volume 1, Overview, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1500-201. <https://doi.org/10.6028/NIST.SP.1500-201>
- [19] Johnson A, Dempsey K, Ross R, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128. <https://doi.org/10.6028/NIST.SP.800-128>
- [20] Barker E, Chen L, Roginsky A, Vassilev A, Davis R (2019) Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56A, Rev. 3. <https://doi.org/10.6028/NIST.SP.800-56Ar3>

- [21] Committee on National Security Systems (2015) Committee on National Security Systems (CNSS) Glossary. (National Security Agency, Ft. Meade, MD), CNSS Instruction (CNSSI) No. 4009. Available at <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>
- [22] Souppaya M, Scarfone K (2013) Guide to Enterprise Patch Management Technologies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 3. <https://doi.org/10.6028/NIST.SP.800-40r3>
- [23] International Organization for Standardization (ISO) 9000:2015, Quality management systems – Fundamentals and vocabulary, September 2015.

698

699 Appendix A—Acronyms

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

701	CSF	Cybersecurity Framework
702	FISMA	Federal Information Security Modernization Act
703	IoT	Internet of Things
704	ITL	Information Technical Laboratory
705	LTE	Long-term Evolution
706	NIST	National Institute of Standards and Technology
707	OMB	Office of Management and Budget
708	OT	Operational Technology
709	RMF	Risk Management Framework
710	SP	Special Publication
711	UWB	Ultrawide Band

712

713 **Appendix B—Glossary**

Capabilities Catalog	Comprehensive list of device cybersecurity capabilities derived from analysis of comprehensive list of source documents for the application or sector. For the federal sector, NIST SP 800-53 Rev. 5 <i>Security and Privacy Controls for Information Systems and Organizations</i> provided the definition of controls used to generate the NIST generated capabilities catalog used for the Federal profile.
Configuration [19, Adapted]	The possible conditions, parameters, and specifications with which an information system or system component can be described or arranged. The Device Configuration capability does not define which configuration settings should exist, simply that a mechanism to manage configuration settings exists.
Core Baseline	A set of technical device capabilities needed to support common cybersecurity controls that protect the customer’s devices and device data, systems, and ecosystems.
Customer [23]	The organization or person that receives a product or service.
Device Cybersecurity Capability	Cybersecurity features or functions that computing devices provide through their own technical means (i.e., device hardware and software).
Device Cybersecurity Capability Core Baseline	See <i>core baseline</i> .
Device Identifier [20, Adapted]	A context-unique value—a value unique within a specific context—that is associated with a device (for example, a string consisting of a network address).
Entity	A person, device, service, network, domain, manufacturer, or other party who might interact with an IoT device.
Federal Profile	Profile of the IoT device cybersecurity capability core baseline [14] and non-technical supporting capability core baseline [15] to provide security guidance provided to federal government organizations related to IoT devices.
Interface [21, Adapted]	A boundary between the IoT device and entities where interactions take place. There are two types of interfaces: network and local.
Local Interface	An interface that can only be accessed physically, such as a port (e.g., USB, audio, video/display, serial, parallel, Thunderbolt) or a removable media drive (e.g., CD/DVD drive, memory card slot).
Network Interface	An interface that connects the IoT device to a network.

Non-Technical Supporting Capability	Non-technical supporting capabilities are actions an organization performs in support of the cybersecurity of an IoT device.
Non-Technical Supporting Capability Core Baseline	The non-technical supporting capability core baseline is a set of non-technical supporting capabilities generally needed from manufacturers or other third parties to support common cybersecurity controls that protect an organization's devices as well as device data, systems, and ecosystems.
Profile	A profile is a baseline set of minimal cybersecurity requirements for mitigating described threats and vulnerabilities, as well as supporting compliance requirements for a defined scope and type of a particular use case (e.g., industry, information system(s)), using a combination of existing cybersecurity guidance, standards and/or specifications baseline documents or catalogs. A profile organizes selected guidance, standard(s) and/or specification(s) and may narrow, expand and/or otherwise tailor items from the starting material to address the requirements of the profile's target application.
Software [6, Adapted]	Computer programs and associated data that may be dynamically written or modified during the device's execution (e.g., application code, libraries).
Update [22, Adapted]	A patch, upgrade, or other modification to code that corrects security and/or functionality problems in software.