Foundational Cybersecurity Activities for IoT Product Manufacturers

Second Public Draft

Michael Fagan
Katerina N. Megas
Barbara Cuthill
Jeffrey Marron
Brad Hoehn

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Foundational Cybersecurity Activities for IoT Product Manufacturers

Second Public Draft

Michael Fagan
Katerina N. Megas
Barbara Cuthill
Jeffrey Marron
Applied Cybersecurity Division
Information Technology Laboratory

Brad Hoehn
HII

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

NIST Technical Series Policies
[Copyright, Use, and Licensing Statements](#)
[NIST Technical Series Publication Identifier Syntax](#)

Publication History
Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added to final publication.]

Author ORCID iDs
Michael Fagan: 0000-0002-1861-2609
Katerina N. Megas: 0000-0002-2815-5448
Barbara Cuthill: 0000-0002-2588-6165
Jeffrey Marron: 0000-0002-7871-683X

Initial Public Comment Period
September 30, 2025 – October 31, 2025

Submit Comments
iotsecurity@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/ir/8259/r1/2pd, including related content, potential updates, and document history.

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

1 Abstract

Internet of Things (IoT) products often lack product cybersecurity capabilities their customers—organizations and individuals—can use to help mitigate their cybersecurity risks. Manufacturers can help their customers by improving the securability of their IoT products by providing necessary cybersecurity functionality and by providing customers with the cybersecurity-related information they need. This publication describes recommended activities related to cybersecurity that manufacturers should consider performing before their IoT products are sold to customers. These foundational cybersecurity activities can help manufacturers lessen the cybersecurity-related efforts needed by customers, which in turn can reduce the prevalence and severity of compromises.

11 Keywords

cybersecurity risk; Internet of Things (IoT); manufacturing; risk management; risk mitigation; securable computing devices; software development

14 **Executive Summary**

15 Manufacturers are creating an incredible variety and volume of internet-ready products and
16 systems broadly known as the Internet of Things (IoT). Many of these IoT products and systems
17 do not fit the standard definitions of information technology (IT) (e.g., smartphones, servers,
18 laptops) that have been used as the basis for defining product cybersecurity capabilities.

19 The purpose of this publication is to give manufacturers recommendations for improving the
20 *securability* of their IoT products. Securability means the IoT products offer *product*
21 *cybersecurity capabilities*—cybersecurity features or functions that the IoT devices and other
22 product components provide through their own technical means (i.e., hardware and software)
23 or related non-technical services from the manufacturer (i.e., vulnerability disclosure
24 programs). An IoT product that is resilient to attacks, supports forensic analysis following an
25 incident, recovers quickly after an incident, keeps customer data confidential and free of
26 tampering, develops a reputation of being trustworthy, etc. is one that customers can adopt
27 and trust. Thus, investing in producing a secure IoT product contributes to the success of the
28 IoT product in the market, increasing innovation, protecting the nation, and supporting
29 individuals in their daily lives. Cybersecurity of an IoT product must begin in the product
30 planning phase when the decision-makers are able to allocate resources towards modeling and
31 prioritizing threats, then designing and implementing effective product cybersecurity
32 capabilities that help address these threats. Additionally, allocating resources for post-market
33 support of the product when it's deployed in the field goes a long way to establishing a
34 relationship of trust with the customer. Constantly evaluating the ever-changing threat
35 landscape, investigating security incidents, and maintaining the IoT product's ability to remain
36 securable in the field all help the customer manage their cybersecurity risks while also
37 enhancing the reputation of the IoT product and its manufacturer.

38 This publication describes nine recommended foundational cybersecurity activities that
39 manufacturers should consider performing to improve the securability of their IoT products. Six
40 of the activities primarily impact decisions and actions performed by the manufacturer before a
41 product is sent out for sale (pre-market), and the remaining three activities primarily impact
42 decisions and actions performed by the manufacturer after product sale (post-market).
43 Performing all activities can help manufacturers provide IoT products that better support the
44 cybersecurity-related efforts needed by customers, which can reduce the prevalence and
45 severity of IoT product compromises. These activities are intended to fit within a
46 manufacturer's existing development process and may already be achieved in whole or part by
47 that existing process. They are presented sequentially and are mostly intended to be performed
48 sequentially, but some activities and parts of activities may be able to be performed in parallel.
49 Also, activities are not mapped to an organizational structure, and in practice these activities
50 may touch on the roles and responsibilities of multiple individuals and departments within an
51 IoT product manufacturer's organization. This allows flexibility for organizations with different
52 structures to adopt the activities and assign them appropriately within their organization. By
53 the end of each activity, IoT product manufacturers will have an increasingly detailed and
54 informed plan to ensure the IoT product they are developing is securable by customers.

55 **Table of Contents**

90   **List of Figures**

102

103 **Acknowledgments**

104 The authors wish to thank all contributors to this publication, including the participants in
105 workshops and other interactive sessions; the individuals and organizations from the public and
106 private sectors, including manufacturers from various sectors as well as several manufacturer
107 trade organizations, who provided feedback.

108 **1. Introduction**

109 Manufacturers are creating an incredible variety and volume of internet-ready products and
110 systems broadly known as the Internet of Things (IoT). Many of these IoT products and systems
111 do not fit the standard definitions of information technology (IT) (e.g., smartphones, servers,
112 laptops) that have been used as the basis for defining product cybersecurity capabilities. IoT
113 products are frequently expected to be in service for decades, may have strict cost limits, could
114 utilize an unorthodox operating environment (e.g., extreme temperatures, high humidity,
115 significant latency) that may affect their cybersecurity posture and expectations.

116 As IoT adoption has increased over the last two decades, threats and vulnerabilities have also
117 grown. For example, large, resilient botnets made up of compromised IoT devices (e.g., the
118 Mirai botnet) resulted in a response from the United States Government in the form of
119 Executive Order (EO) 13800. [1] Since that time, there's been increasing acknowledgement of
120 the importance of cybersecurity of IoT products and efforts to support and promote it. [2] Even
121 today, trust in IoT, which is supported by cybersecurity, is seen as a key factor to sustaining and
122 amplifying the adoption and innovation of IoT products. [3] Manufacturers should consider the
123 cybersecurity of their IoT products to ensure customers can trust the products and their
124 operation. Doing so can not only protect customers as they deploy and use IoT products, but
125 manufacturers themselves by increasing trust in their products, supporting their reputation
126 among customers, and reducing the likelihood of attacks on manufacturers' internal systems.
127 Finally, considering cybersecurity in the development and support of IoT products protects the
128 Nation, Internet, and public at large by reducing the likelihood of attacks utilizing IoT products
129 (e.g., botnets).

130 **1.1. Purpose and Scope**

131 **IoT products** are digital equipment or systems that sense or actuate on the physical world while
132 being connected or connectable to the Internet. IoT products in scope for this publication may
133 be comprised of a single IoT device and nothing else or they may be comprised of the IoT device
134 and additional **IoT product components** (e.g., backends, companion applications, and specialty
135 networking/gateway hardware). An **IoT device** has at least one transducer (sensor or actuator)
136 for interacting directly with the physical world and at least one network interface (e.g.,
137 Ethernet, Wi-Fi, Bluetooth, Long-Term Evolution (LTE), Zigbee, Ultra-Wideband (UWB)) for
138 interfacing with the digital world. In this document, "components" refers to the components of
139 an IoT product. Sub-components of an IoT device (e.g., a processor or memory) are outside the
140 scope of this publication.

141 IoT product customers will have **needs and goals**, which is defined as their desires and
142 objectives in operating their systems. Some of these needs and goals will be related to
143 cybersecurity. For a business or other organization, their needs and goals would be their
144 business mission and objectives, and they may have cybersecurity needs and goals that could
145 be expressed as a profile of the NIST Cybersecurity Framework (CSF) or be driven by
146 regulations, standards, and industry best-practices. Other customers, such as individuals using

147 IoT products in their home will also have needs and goals, including those for cybersecurity, but
148 would not generally use tools like the CSF to express them and may not have applicable
149 regulations, standards, and industry best-practices to rely on.

150 The purpose of this publication is to provide manufacturers recommendations for developing
151 **securable** IoT products. Securable means that the IoT products operate in a way and offer
152 functionality such that a customer (or other users) can effectively manage the cybersecurity of
153 the IoT product and the system to which it's connected. In other words, a securable IoT product
154 is one that supports customers' cybersecurity needs and goals. This publication provides
155 guidelines for securable IoT products rather than *secure* IoT products because:

156 1. When considering that IoT products will be attached to networks and primarily managed by
157   customers when deployed, IoT product manufacturers cannot create something that is
158   secure in an absolute sense, but rather securable by customers in deployment.

159 2. Secure operation of IoT products is only part of the scope of this document, and this
160   document also addresses how IoT products should support the cybersecurity of customers
161   and the systems they attach to.

162 IoT products will offer *product cybersecurity capabilities* that customers, including both
163 organizations and individuals, need to secure the IoT products when used in their systems and
164 environments. While all customers may need to take some actions to secure their IoT products
165 (e.g., changing a default password), product cybersecurity capabilities will need to be tailored
166 to the expected knowledge of the customer. All IoT product components will contribute to the
167 securability of IoT products, and so product cybersecurity capabilities will include aspects of
168 how IoT products function that ensure secure operation of the IoT product but may not be used
169 directly by customers. For example, confidentiality measures such as encryption should be part
170 of the IoT product's implementation to protect data-at-rest and data-in-transit, even for data
171 that is stored on and shared between IoT product components.

172 Finally, IoT product manufacturers or other supporting entities will often need to perform
173 actions or provide services that their customers need to maintain the cybersecurity of the
174 product. From this publication, IoT product manufacturers will learn how they can help IoT
175 product customers with cybersecurity risk management by carefully considering which product
176 cybersecurity capabilities to design into their products and which actions or services may also
177 be needed to support the IoT product's securability.

178 Therefore, a **securable IoT product** has product cybersecurity capabilities provided over the
179 expected life of the product by the manufacturer or other supporting entity that customers
180 may need to mitigate common and expected cybersecurity risks related to the use of the IoT
181 product and its connection to customers' systems.

182 This publication is intended to address a wide range of IoT use cases. IoT products will be used
183 in systems and environments with many other products and system components, some of
184 which may be IoT, while others may be conventional IT equipment. For some use cases (e.g.,
185 healthcare), the guidelines in this document can be complimented with applicable standards,
186 regulations, and guidance.

187 This publication is primarily intended to inform the manufacturing of new devices and products
188 or products that are being redesigned. However much of the information in this publication can
189 be used when upgrading products already in production. By implementing the activities
190 discussed in this document, manufacturers can increase the securability of the IoT products
191 they produce, thus improving the manufacturer's reputation and contributing to the success of
192 the deployment.

193 Readers do not need a technical understanding of IoT product composition and capabilities, but
194 a basic understanding of cybersecurity principles is assumed.

195 **1.2. Publication Structure**

196 The remainder of this publication is organized into the following sections and appendices:

197 • Section 2 provides background information needed to understand the seven recommended
198   pre-market and post-market activities described in Sections 3 and 4.

199 • Section 3 includes recommended manufacturer activities that primarily impact securability
200   efforts by the manufacturer before sale (i.e., premarket). The Section 3 activities are:

201   o Activity 0: Prioritize Cybersecurity and Maintain Cybersecurity Posture.

202   o Activity 1: Identify Expected Customers and Define Expected Use Cases.

203   o Activity 2: Research Customer Cybersecurity Needs and Goals.

204   o Activity 3: Determine Appropriate Means to Support Customer Needs and Goals in
205   the Context of the IoT Product.

206   o Activity 4: Define IoT Product Cybersecurity Capabilities Based on Appropriate
207   Means.

208   o Activity 5: Plan for Adequate Support of Customer Needs and Goals.

209 • Section 4 includes recommended manufacturer activities that primarily impact securability
210   efforts by the manufacturer after sale (i.e., post-market). The Section 4 activities are:

211   o Activity 6: On-Going Support of Product Cybersecurity through-out the Lifecyle and
212   through End-of-Life.

213   o Activity 7: Define Approaches for Communicating to Customers.

214   o Activity 8: Decide What to Communicate to Customers and How to Communicate It.

215 • Section 5 provides a conclusion for the publication.

216 • The References section lists the references for the publication.

217 • Appendix A provides a list of acronyms and abbreviations used in the publication.

218 • Appendix B contains a glossary of selected terms used in the publication.

219 • Appendix C presents changes that were made to the original NIST IR 8259 report in writing
220   this Initial Public Draft.

221 **2. Background**

222 This section provides an overview of the background concepts needed to understand the rest of
223 the publication.

224 **2.1. Product Cybersecurity and System Cybersecurity**

225 The following discussion uses NIST's prior work on cybersecurity such as the NIST Cybersecurity
226 Framework (CSF) and Risk Management Framework (RMF). The intent is not to suggest all IoT
227 product manufacturers must consider cybersecurity from the same perspective as large
228 enterprise organizations or the federal government. These frameworks are adaptable to a
229 broad range of organizations. The point of using these frameworks is to clarify the perspective
230 on cybersecurity used in this publication that should be considered by all IoT product
231 manufacturers: product cybersecurity.

232 NIST guidelines, including this publication, take a risk-based approach to cybersecurity. In this
233 context, cybersecurity risk is defined by the RMF as "a measure of the extent to which an entity
234 is threatened by a potential circumstance or event, and typically a function of: (i) the adverse
235 impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of
236 occurrence." [4] In general, cybersecurity risks are "those risks that arise from the loss of
237 confidentiality, integrity, or availability of information or information systems and reflect the
238 potential adverse impacts to organizational operations (including mission, functions, image, or
239 reputation), organizational assets, individuals, other organizations, and the Nation." [4] As such,
240 tools such as the NIST CSF provide guidelines for organizations to manage cybersecurity risks
241 related to the systems they use. A risk-based approach to system cybersecurity points
242 organizations to consider their system(s) in totality to determine the applicable cybersecurity
243 risks that must be mitigated via cybersecurity controls, which are "the safeguards or
244 countermeasures prescribed for an information system or an organization to protect the
245 confidentiality, integrity, and availability of the system and its information." [5] The controls
246 implemented, outcomes targeted, or other actions taken related to cybersecurity could be
247 generally referred to as an *organization's cybersecurity functionality*.

248
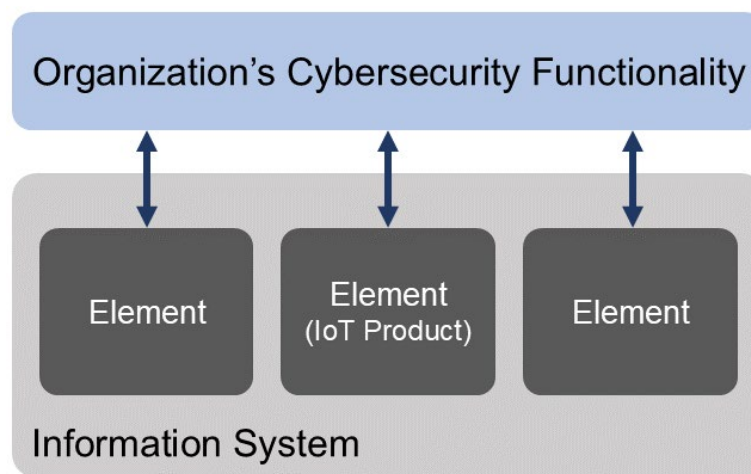
249   **Figure 1:Relationship of organizational information system elements to an organization's cybersecurity.**

250   Manufacturers should take a risk-based approach towards the cybersecurity of the products
251   they make. Although risk-based cybersecurity generally considers the risks faced by an entire
252   information system, manufacturers may produce individual elements that are used with other
253   products to create information systems. This is because systems are created by interconnecting
254   various products such as personal computers, mobile devices, servers, networking equipment,
255   and various peripherals including an increasing number of IoT products with their components
256   (e.g., devices, mobile apps). As shown in Fig. 1, there are dependencies that must be met by
257   elements of an information system in order for cybersecurity functionality to be feasibly or
258   effectively implemented by the manager and owner of the information system. For example,
259   how can access control be enforced if a device on the network does not allow a default
260   password to be changed? In some instances, new controls such as network segmentation can
261   be implemented, but not in all cases and not without additional cost and system complexity.
262   Therefore, there can be value to viewing cybersecurity from the product perspective, which
263   takes into account the relationship of system elements with the overall system, but also the
264   limitations of information that can be known when assessing risks. When taking this product
265   perspective, assessment of risks is limited to those related to the product, while assumptions
266   may have to be made about expected customers and how they secure their systems. This
267   publication provides risk-based cybersecurity guidelines from the product perspective targeted
268   at IoT product manufacturers.

2.2. Composition of IoT Products

270   IoT products can have many compositions. Some may only have an IoT device and may or may
271   not require additional IoT product components to operate, but many IoT products across many
272   use cases require additional components such as backends, companion applications, and
273   specialty networking/gateway hardware. In some use cases, such as home IoT applications, it is
274   common for IoT devices to require other IoT product components to operate, but IoT products
275   in enterprise and industrial use cases can also utilize multi-component IoT product designs. The
276   need for additional IoT product components to support an IoT device can be driven by
277   operational needs. For example, an IoT device may lack the ability to accommodate an
278   appropriate human-user interface. In that situation, individuals will often have to interact with
279   a companion application that is installed on a smartphone.

280

281   **Figure 2:Example of a network showing multiple IoT products based around different IoT devices which are**
282   **supported by various kinds of IoT product components.**

Fig. 2 shows how IoT product architectures can vary when viewed in an example deployment environment. Two different IoT products are shown with different IoT devices that both utilize a backend but use different architectures to do so: one IoT device (i.e., the orange television) connects directly to the deployment environments' networking re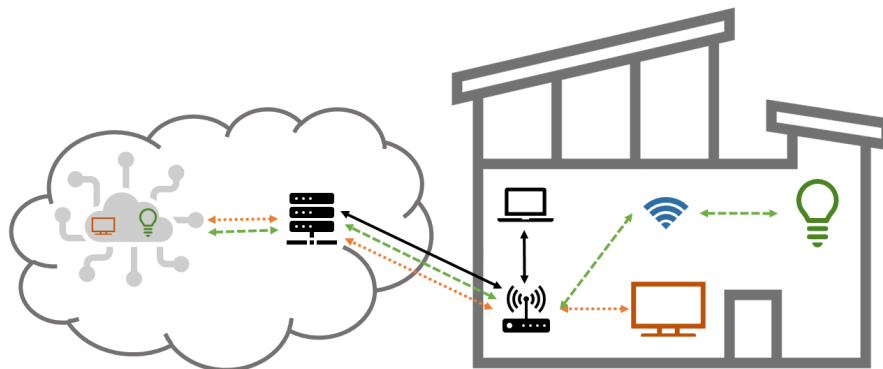sources while the other (i.e., the green light bulb) utilizes a specialty gateway to convert data from the device into networking packets for transmission. While the IoT devices, backends, and networking hardware specific to an IoT product would all be considered IoT product components of their respective products, other equipment (e.g., networking equipment), though used by IoT product components, are not considered IoT product components. Beyond networking equipment, other devices will likely be present on the network that would also not be considered IoT product components. That said, some of these devices (e.g., personal computers, smartphones) may host IoT product components (e.g., mobile apps) in the form of application code used to interface with the product.

Determining which components are part of an IoT product and which are not should be driven by whether removal of or disconnection from the component would break IoT product functionality. For example, a manufacturer that designs an IoT product with a device requiring a connection to software hosted in a backend cloud to function should consider that backend as part of the IoT product. IoT product components can take any form of hardware or software, but most IoT product components will fit one of the following descriptions:[1]

- IoT device – local equipment with at least one transducer (i.e., sensor or actuator) and at least one network interface.

- Specialty networking/gateway hardware – local equipment used to aggregate, translate, forward, or distribute data related to the IoT product across networks (e.g., a hub within the system where the IoT device is used).

- Companion application software – code executed on local equipment outside of the IoT product boundary (e.g., personal computer, smartphone) that interfaces with other IoT product components (e.g., a mobile app for communicating with the IoT device).

- Backends – remote service that supports one or more IoT product components (e.g., a cloud service, or multiple services, that may store and/or process data from the IoT device).

2.3. Entities in an IoT Product Ecosystem

All technology, including IoT products, is created for practical purposes, namely to provide entities with some utility. *Entities* are individuals or organizations, and with respect to IoT products, there are several entities to consider. Manufacturers, sometimes referred to as developers, are entities who create IoT products from hardware and software. Customers are entities who use IoT products. Other entities include, but are not limited to:

---

[1] NIST has published other guidelines that provide additional perspectives and models for describing IoT product components and how they work together to provide IoT product functionality, including the *Internet of Things (IoT) Component Capability Model for Research Testbed*, NIST IR 8316 [6], and *'Network of 'Things,'* SP 800-183. [7]

- Suppliers – These entities sell or otherwise provide resources, hardware, software, etc. to other entities. For example, big box stores, online retailers, small electronic boutique stores are suppliers of home IoT products. Sometimes, manufacturers may be suppliers as well if they directly sell to other entities. Manufacturers will also acquire resources, hardware, software, etc. from suppliers to develop and produce IoT products as part of their supply chain.

- Installer – These entities deploy hardware, software, etc. into their operational environments. For example, building management and security systems may be deployed by professional technicians who select and deploy IoT and other products throughout a building. Installers may be performing these actions on their own behalf or as a service for others.

- Maintainer – These entities maintain the hardware and software in the IoT product. For software this would include taking information about newly discovered vulnerabilities and providing software updates or other recommendations to maintain the cybersecurity of the product. For hardware, this would include maintaining the physical integrity of the device including replacing any failing elements.

IoT product ecosystems can be complex and include many different entities. Note that entities could be organizations or individuals. Also, entities in the ecosystem may not always be introduced by any direct action but could become part of the IoT product's ecosystem by happenstance or necessity. There may be instances in which an individual other than the customer may be introduced to the IoT product's ecosystem. One example includes individuals that interact with the IoT product, even if the interaction is limited to being the subject of a sensor or involved in an actuation. In practical terms, this could include individuals who enter a space where the owner of the space has deployed IoT cameras that record and process data on all individuals in the space. There may also be organizational entities introduced to an IoT product's ecosystem by necessity, such as when an IoT product employs the Matter protocol, which allows IoT products from different manufacturers to interoperate and share backend support.

Not all entities that interact with IoT products necessarily have the same impact on and relationship with cybersecurity related to the IoT product. Generally, the further from the customer-manufacturer nexus an entity lies, the less impact those entities will have on the IoT product's cybersecurity. Direct entities, such as those brought into the IoT product's ecosystem by the customer (e.g., other explicit IoT product users) and the manufacturer (e.g., IoT product component developers) will have more impact than the indirect entities discussed in the previous paragraph. With their central role in developing an IoT product, manufacturers have significant opportunity to impact securability.

2.4. The Role of the Manufacturer in Cybersecurity

The *pre-market* phase of an IoT product's life encompasses what the manufacturer does *before* the product is marketed and sold to customers. Any actions the manufacturer takes for an IoT product after it is sold, such as addressing vulnerabilities, delivering updated or new

358   capabilities, or providing cybersecurity information to customers, are considered part of the
359   *post-market* phase. Manufacturers are generally best able to identify and incorporate plans for
360   the product cybersecurity capabilities their product will have early in the pre-market phase.

361   Manufacturers should consider cybersecurity, including selecting product cybersecurity
362   capabilities, as early in the pre-market phase as possible. Delaying decisions about product
363   cybersecurity capabilities to later in the pre-market phase can create difficulty since making
364   design or implementation changes is usually more complicated, costly, and potentially delay the
365   product launch. Once a product is on the market, many cybersecurity changes may no longer be
366   viable because of hardware constraints, and those that are viable may be much more difficult
367   than if they had been done pre-market. Manufacturers may still have a role in the securability
368   of their IoT products during the post-market phase by providing or ensuring other supporting
369   entities provide non-technical supporting capabilities.

370   Sections 3 and 4 of this publication describe cybersecurity activities and related planning that
371   manufacturers should consider performing when developing and supporting their IoT products.
372   Section 3 covers activities that primarily impact the pre-market phase, while Section 4 discusses
373   activities that primarily impact the post-market phase. The activities in Sections 3 and 4 focus
374   on key cybersecurity activities and represent a subset of what manufacturers may need to do
375   during their product development process and are not intended to be comprehensive. For
376   example, manufacturers will also find it easier to design and produce securable IoT products if
377   they ensure their workforce has the necessary skills to perform the activities.

378   **Table 1. Recommended manufacturer activities discussed in this publication.**

	Activity	Example Output
Pre-Market Phase	Activity 0: Prioritize Cybersecurity and Maintain Cybersecurity Posture	*A secure organizational network, development process, and culture*
	Activity 1: Identify Expected Customers and Define Expected Use Cases	*List of expected customers of the IoT product; report of how customers are expected to use the product*
	Activity 2: Research Customer Cybersecurity Needs and Goals	*An understanding of customer cybersecurity needs and goals; standards and other documents that express the customer needs and goals*
	Activity 3: Determine Appropriate Means to Support Customer Needs and Goals	*Insights into appropriate means to support customers' cybersecurity needs and goals; conception of known requirements that could impact appropriate means, such as physical product constraints or conflicting customer expectations*

	Activity 4: Define IoT Product Cybersecurity Capabilities Based on Appropriate Means	*List of IoT product cybersecurity capabilities that could be defined by appropriate means, even if means or use of means vary for different customers or use cases*
	Activity 5: Plan for Adequate Support of Customer Needs and Goals	*List of hardware and software needed to support device cybersecurity capabilities; plans and procedures to implement non-technical capabilities*
	Product Goes to Market	*IoT product for sale or sold*
Post-Market Phase	Activity 6: On-Going Support of Product Cybersecurity through-out the Lifecyle End-of-Life	*Active vulnerability remediation program; available product support*
	Activity 7: Define Approaches for Communicating to Customers	*List of communication methods appropriate for cybersecurity context related to the IoT product*
	Activity 8: Decide What to Communicate to Customers and How to Communicate It	*Regular customer notifications; regulatory and other applicable disclosures*

379

380   Table 1 shows the foundational cybersecurity activities covered in this publication, arranged by
381   the phase in which the activity's output will primarily impact product securability. Example
382   outputs are provided for each of the recommended activities. As indicated in the table,
383   activities highlighted for each phase build on each other within that phase such that each pre-
384   market activity will build on the outcomes of prior activities. While the activities recommended
385   for the post-market phase may use artifacts and outcomes from pre-market activities, they may
386   also draw on other information sources. The moment at which a product is considered to have
387   "gone to market" will vary by use case, manufacturer, and circumstance, but is defined as when
388   the IoT device associated with the IoT product is no longer under the control of the
389   manufacturer (i.e., when it has been released to an intermediary, such as a retailer, or to end-
390   customers). Activities primarily impacting the post-market phase, though intended to help the
391   securability of IoT products after or as they are sold (e.g., by helping inform customers how a
392   device can help meet their cybersecurity needs and goals, which may or may not include risk
393   mitigation goals), should be planned for during the pre-market phase.

394   **2.5. IoT Product Customer Cybersecurity Needs and Goals**

395   Improving the securability of an IoT product means helping customers meet their cybersecurity
396   needs and goals. All customers will have cybersecurity needs and goals, but the specific
397   cybersecurity needs and goals for a customer of an IoT product will be dependent on the

398 threats faced by the product and risks potentially associated with the product. The needs and
399 goals will also be framed and informed by the customer's knowledge, expectations, etc.
400 Addressing cybersecurity needs and goals should be risk-based. Even customers without formal
401 risk mitigation goals, such as home consumers, will care about cybersecurity threats and often
402 have informal and indirect cybersecurity goals. At the least, customers will want their IoT
403 products to provide desired functionality as expected (e.g., automatically), which is dependent
404 on addressing threats the product faces that could impact functionality.

405 Risk-based cybersecurity guidelines intended to be used by customers can provide insights into
406 cybersecurity needs and goals for customers. Based on an analysis of existing NIST publications
407 such as SP 800-53 [5] and the Cybersecurity Framework [8] and the characteristics of IoT
408 devices, NIST IR 8228 [9] presents common enterprise risk mitigation areas (e.g., access
409 management, data protection, vulnerability management), and thus common cybersecurity
410 needs and goals for IoT product customers:

411 • **Asset Management:** Maintain a current, accurate inventory of all IoT products and their
412   relevant characteristics throughout the products' lifecycles[2] in order to use that information
413   for cybersecurity risk management purposes. Being able to distinguish each IoT product
414   deployment from all others is needed for the other common risk mitigation areas, such as
415   vulnerability management, access management, data protection, and incident detection.

416 • **Vulnerability Management:** Identify and mitigate known vulnerabilities in the software of
417   IoT devices and other IoT product components throughout the IoT products' lifecycles in
418   order to reduce the likelihood and ease of exploitation and compromise. Vulnerabilities can
419   be eliminated by installing updates (e.g., patches) and changing configuration settings.
420   Updates can also correct IoT product operational problems, which can improve availability,
421   reliability, performance, and other aspects of product operation. Customers often want to
422   alter configuration settings for a variety of reasons, including improving or customizing
423   cybersecurity, interoperability, privacy, and usability features. Criticality is important to
424   consider with respect to vulnerabilities since critical vulnerabilities may necessitate a
425   temporary mitigation for customers while an update is developed.

426 • **Access Management:** Prevent unauthorized and improper physical and logical access to,
427   usage of, and administration of IoT products throughout their lifecycles by people,
428   processes, and other computing devices. This includes limits on access privileges for the
429   manufacturer themselves, as well as other entities who may interact with the IoT product
430   such as bystanders and maintainers. Following the principle of least privilege, all authorized
431   entities should have a clear and distinct purpose for access, and their access should be
432   strictly limited to what is necessary for the purpose. Limiting access to interfaces reduces
433   the attack surface of the product, giving attackers fewer opportunities to compromise it.
434   For the IoT device component of the product, this includes physical interfaces.

---

[2] IoT product lifecycles can differ. Some software components may no longer be maintained or supported creating an end-of-life for the IoT product as a connected product while the mechanical components of the product may continue to be functional. (For example, a smart refrigerator may continue to keep the contents cold even if the smart features are no longer maintained or no longer function.)

435 • **Data Protection:** Prevent access to and tampering with data at rest or in transit that might
436   expose sensitive information or allow manipulation or disruption of IoT product operations
437   throughout the lifecycle including at disposal.

438 • **Incident Detection:** Monitor and analyze IoT product activity for signs of incidents involving
439   data security across IoT products' components and throughout the products' lifecycles.
440   These signs can also be useful in investigating compromises and troubleshooting certain
441   operational problems.

442 Sections 3 and 4 of NISTIR 8228 [9] discuss additional cybersecurity-related considerations that
443 manufacturers should be mindful of when identifying the product cybersecurity capabilities
444 that IoT products should provide. Also, Tables 1 and 2 in Section 4 of NISTIR 8228 list common
445 shortcomings in IoT cybersecurity and explain how they can negatively impact customers. The
446 discussion in NISTIR 8228 provides the rationale for each capability in the core baselines
447 defined in the companion publications, NISTIR 8259A, *IoT Device Cybersecurity Core Baseline*
448 [10] and NISTIR 8259B, *IoT Non-Technical Supporting Capability Core Baseline*. [11]

449 For many IoT products, additional types of risks, such as privacy,[3] safety,
450 reliability, or resiliency, need to be managed simultaneously with
451 cybersecurity risks because addressing one type of risk can have
452 impacts on others. A common example is ensuring that when a product
453 fails, it does so in a safe manner. Only cybersecurity risks are discussed
454 in this publication. Readers who are interested in better understanding
455 other types of risks and their relationship to cybersecurity may benefit
456 from reading NIST SP 800-82 Revision 2, *Guide to Industrial Control*
457 *Systems (ICS) Security* [12] and NIST SP 1500-201, *Framework for Cyber-*
458 *Physical Systems: Volume 1, Overview, Version 1.0* from the Cyber-
459 Physical Systems Public Working Group. [13]

460 **2.6. Relationships between Needs and Goals, Capabilities, and Means**

461 Manufacturers of IoT products can help address cybersecurity needs and goals by incorporating
462 corresponding product cybersecurity capabilities into their IoT products. In turn, customers
463 should have fewer challenges in securing those products since IoT product cybersecurity
464 capabilities will better align with customer expectations. Many of the risk mitigation areas
465 identified in Sec. 2.5 can only be addressed effectively, and most are addressed more
466 efficiently, by manufacturers building product cybersecurity capabilities into products instead
467 of customers providing cybersecurity risk mitigations in the deployment environments. Many
468 customers do not have the resources or expertise to mitigate risks absent the manufacturer
469 building comprehensive product cybersecurity capabilities into their products.

470 In practice, customers will use means to achieve their needs and goals. Means is defined as "an
471 agent, tool, device, measure, plan, or policy for accomplishing or furthering a purpose." [14]

---

[3] While the device cybersecurity capability core baseline includes product cybersecurity capabilities that also support privacy, such as protecting
the confidentiality of data, it does not include non-cybersecurity related capabilities that support privacy.

472   This publication refers to technical or non-technical means for cybersecurity purposes, whether
473   performed by an IoT product itself or from supporting entities. Customers will rely on these
474   means to plan for and maintain the cybersecurity of the product within their systems and
475   environments. Fig. 4 depicts how various kinds of means, implemented by different IoT product
476   components and ecosystem entities comprise product cybersecurity capabilities.

477
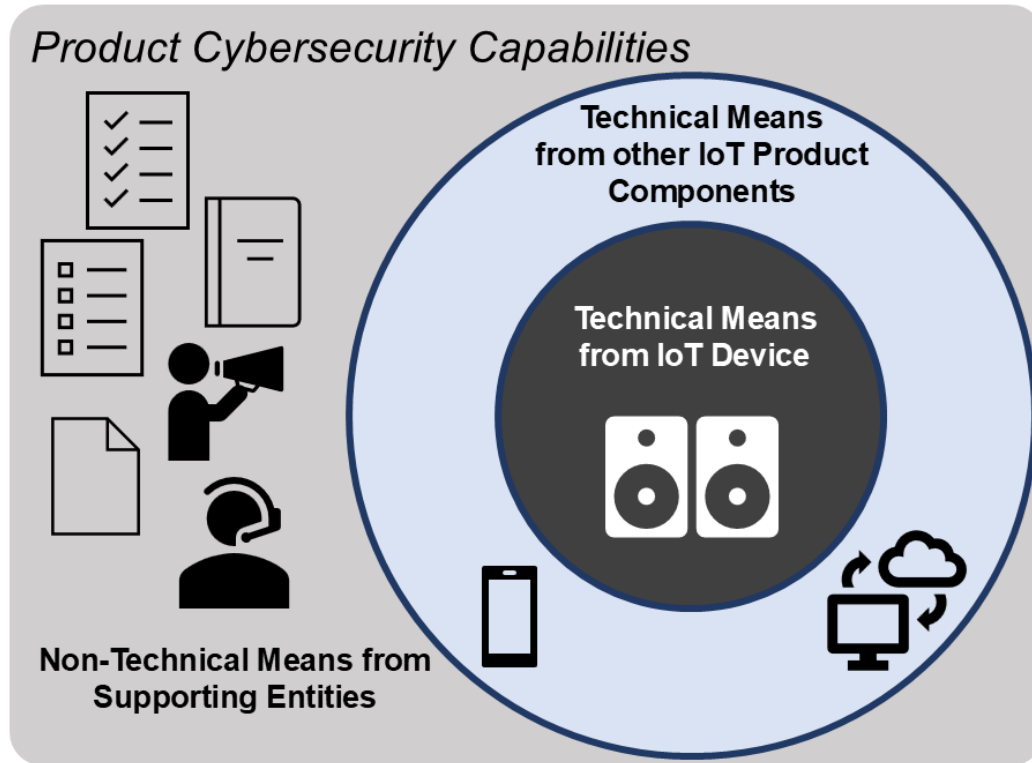
478   **Figure 3:Technical and non-technical means that can support cybersecurity of IoT products provided as product**
479   **cybersecurity capabilities.**

480   IoT products' technical means (shown within co-centric circles in Fig. 3) will define product
481   cybersecurity capabilities to support the cybersecurity of the networks to which they are
482   eventually attached. In general, NIST has defined a capability as "a combination of mutually
483   reinforcing controls implemented by technical means, physical means, and procedural means."
484   [4] More specifically, product cybersecurity capabilities are capabilities aligned with this
485   definition but provided by or related to the IoT product. IoT device cybersecurity capabilities
486   are capabilities provided by the IoT device specifically (i.e., cybersecurity features or functions
487   the device provides through its own technical means). Other IoT product components may also
488   contribute to IoT product cybersecurity capabilities through their technical means.

489   IoT product components will have different resources and capabilities available and, thus,
490   different ways they will contribute to product cybersecurity capabilities. Some product
491   cybersecurity capabilities will be supported similarly by most IoT product components. For
492   example, data protection will use the same or similar means across IoT product components to
493   protect data at rest and in transit. Other product cybersecurity capabilities may be supported
494   differently by various IoT product components. For example, controlling access to interfaces

495   may use similar means (e.g., passwords) for an IoT device and its backend, but the IoT device
496   may have local interfaces whereas the backend may have remotely accessible interfaces.
497   Finally, some product cybersecurity capabilities may be supported entirely differently by
498   different IoT product components. For example, software updates will be managed on the IoT
499   device through potentially automated systems and the customer; however, backend software
500   updates will be managed by the administrator of the backend.

501   Finally, product non-technical supporting capabilities are procedural means implemented and
502   provided by IoT product manufacturers or other supporting entities that help support
503   cybersecurity. For example, vulnerability reporting and disclosure capabilities implemented by
504   the manufacturer through primarily procedural means would support product cybersecurity.

505   In summary, both technical and non-technical means are used to implement product
506   cybersecurity capabilities, which in turn support customer needs and goals. Table 2 shows three
507   examples of how customer needs and goals can be supported by specific product cybersecurity
508   capabilities along with potential means to define the capabilities.

509   **Table 2: Examples demonstrating relationship among customer needs and goals, product cybersecurity**
510   **capabilities, and means.**

Example Customer Needs and Goals	Supporting Product Cybersecurity Capability	Potential Means
"My data is protected from attacks."	Data Protection – all data at rest and in transit is protected.	The IoT device uses the Advanced Encryption Standard (AES) algorithm to encrypt data when it is stored or before it is sent over communication channels.
"The product will work as I expect."	Software Update – all software is kept up to date.	An over-the-air method is implemented in the IoT device that automatically downloads, verifies via cryptographic signature the update package, and applies the update.
"I can use the product securely and know what capabilities are available."	Product Education and Awareness – the customer is kept aware of and educated about cybersecurity-related information.	A printed manual is included with the IoT product that describes the product cybersecurity capabilities available. A link is provided to a digital version of the product manual detailing the cybersecurity capabilities, hosted and kept updated by the manufacturer.

511

512   Rather than discuss technical and non-technical means exclusively, this publication will also
513   refer to product cybersecurity capabilities and device cybersecurity capabilities. In many cases,
514   technical and non-technical means can be easier to identify to satisfy a customer's
515   cybersecurity needs and goals, but product cybersecurity capabilities allow for the IoT product

516 manufacturer to express how the IoT product supports cybersecurity when the specific means
517 may be indeterminate. For example, product cybersecurity capabilities may be more useful
518 than means to describe the cybersecurity features when different means are used for different
519 customers or deployments. For some entities, including many customers, specific means are
520 immaterial to the product cybersecurity capabilities provided. Finally, in discussion of these
521 concepts for the purposes of this publication, where complete and specific details about IoT
522 products are not possible, it is easier to generalize expectations around cybersecurity at the
523 level of product and device cybersecurity capabilities rather than specific technical and non-
524 technical means. Nonetheless, in all cases where any of these terms are used, readers should
525 keep their relationship in mind.

526 The rest of this publication guides IoT product manufacturers through foundational activities
527 that help them consider cybersecurity related to the IoT products they develop and produce.

528   **3. Manufacturer Activities Impacting the IoT Product Pre-Market Phase**

529   Manufacturers should consider performing the foundational cybersecurity activities described
530   in this section to improve the securability of IoT products for customers (e.g., increase the
531   range or efficacy of customer-expected product cybersecurity capabilities offered in IoT
532   products). The activities should be integrated with a manufacturer's other pre-market activities,
533   and they will primarily impact those other pre-market activities. Many of these activities are
534   likely already taking place and will just need extension to explicitly consider cybersecurity. For
535   example, identifying expected customers and use cases is necessary for determining the
536   operational features and functions of a product and how to market the product, but it is also
537   foundational to determining the cybersecurity risk that needs mitigation. Effort should not be
538   duplicated; artifacts from all pre-market activities can inform cybersecurity-specific actions at
539   any stage. The more integrated these suggested activities are with other pre-market activities,
540   the better cybersecurity is likely to be planned for and implemented in IoT products.

541   **3.1. Activity 0: Prioritize Cybersecurity and Maintain Cybersecurity Posture**

542   Manufacturers of IoT products will likely employ digital technologies to facilitate the design and
543   production of their IoT products. The cybersecurity of the manufacturer's operational
544   environment, as well as the general priority that the manufacturer gives to cybersecurity, can
545   impact the securability of the products they make. Manufacturers can be targets of
546   cyberattacks, and impacts to their systems and organizations can have direct or indirect
547   impacts on the securability of the IoT products they develop. For example, attackers could gain
548   access to the manufacture's internal systems where software development occurs. With this
549   access, they could take several actions that could impact IoT product customers. They may
550   inject malware into the manufacturer's code base, setting up a broader attack utilizing
551   deployed IoT products made by the manufacturer. They could use ransomware to cripple the
552   manufacturer's systems which can in turn halt or slow support for IoT products such as
553   software update development to patch security vulnerabilities.

554   IoT products can also be composed of IoT product components outside customers' control but
555   nonetheless store and process IoT product data. The manufacturer may host these IoT product
556   components themselves, contract with another organization to host the components, or, at the
557   least, engineer their product to function with backends based on some interoperable protocol
558   (e.g., Matter). In any case, the manufacturer's cybersecurity prioritization and posture can
559   impact the subsequent securability of their IoT products. This is clear when the manufacturer
560   hosts the product component themselves and the manufacturer's poor cybersecurity practices
561   could result in stored IoT product data being susceptible to attack. In other cases, the
562   cybersecurity practices and posture of the manufacturer related to secure supply-chain and
563   development practices can influence the securability of the IoT product. For example, a
564   manufacturer that prioritizes adequate cybersecurity practices may have processes
565   implemented to assess the cybersecurity posture of service providers, such as those they
566   contract to host backend IoT product components. Manufacturers that prioritize cybersecurity
567   may also employ secure development practices when designing and developing the hardware

568 and software for their IoT products, including the use of all protocols and protection of IoT
569 product data in any environment possible.

570 Therefore, the other activities discussed in this publication assume this Activity 0 has been
571 taken by manufacturers, and that manufacturers prioritize cybersecurity and maintain their
572 organizational cybersecurity posture. Many manufacturers practice this activity outside the
573 context of development of securable IoT products, but the range of IoT product use cases,
574 variety in composition of IoT product manufacturer organizations, and expertise of
575 organizations' personnel means some organizations may have limited experience with
576 cybersecurity. All manufacturers can benefit from answering the following questions related to
577 their cybersecurity prioritization and maintaining cybersecurity posture:

578 1. **How does my organization identify cybersecurity threats and risks?** Manufacturers can
579   utilize tools such as the MITRE ATT&CK or EMB3D Frameworks to identify applicable threats
580   to both their operations and systems, as well as to their IoT products in deployment.

581 2. **How does my organization assess and mitigate cybersecurity risks we face?** It is critical
582   that IoT product manufacturers aim for a strong cybersecurity posture by proactively
583   protecting their operations and systems from cybersecurity attacks. Many standards and
584   other tools exist to aid organizations, including IoT product manufacturers, in the
585   assessment of cybersecurity risk and selection of appropriate mitigations. For example,
586   organizations can look to the Cybersecurity Framework (CSF), Risk Management Framework
587   (RMF), and the ISA/IEC 62443 series, to name a few.

588 3. **What are effective means that my organization can use to monitor for potential
589   cybersecurity attacks and detect when a cybersecurity attack may be underway?** Risk
590   management is an on-going process, and so manufacturers should implement cybersecurity
591   controls that help them monitor their operations and systems and identify signs of
592   cybersecurity attacks.

593 4. **When there is a cybersecurity attack, what are my organization's response and recovery
594   plans?** Cybersecurity attacks are not always stopped by existing controls, and so
595   manufacturers should be prepared to respond and recover from their impacts. For example,
596   regularly backing up systems and their data can help an organization respond to a
597   ransomware attack or natural disaster.

598 5. **What are ways all parts of my organization contribute to our cybersecurity posture?**
599   Cybersecurity should not be siloed to one team or division. Organizations run on digital
600   technologies, and so cybersecurity should be considered across all units.

601 6. **Are there cybersecurity considerations for my organization based on our role as an IoT
602   product developer and manufacturer?** Cybersecurity considerations for developers and
603   manufacturers can be distinct in some ways from cybersecurity considerations for
604   organizations in general. Tools such as the Secure Software Development Framework (SSDF)
605   [15] can help software developers, including IoT product manufacturers. Cybersecurity of
606   the supply-chain for an IoT product, including portions of the development or support of
607   the IoT product by other parties, is also important for IoT product manufacturers to
608   consider. Manufacturers can refer to *Cybersecurity Supply Chain Risk Management Practices*

609   *for Systems and Organizations*, SP 800-161 Rev. 1 [16] for additional information about
610   supply-chain risk management.

611 The rest of the foundational activities concern the cybersecurity of IoT products rather than the
612 cybersecurity posture of IoT manufacturers. As the designer of equipment customers will use
613 and potentially rely on, IoT product manufacturers have a critical role in the cybersecurity of
614 the IoT products they produce. Though manufacturers can understand the impacts of
615 cybersecurity attacks against their own operations and systems, it can be more difficult for
616 them to gain awareness of and consider impacts to other entities, including customers. The
617 subsequent foundational activities in this publication guide IoT product manufacturers through
618 cybersecurity considerations related to their products that require them to focus on the
619 cybersecurity of their customers.

620 **3.2. Activity 1: Identify Expected Customers and Define Expected Use Cases**

621 Manufactures should look to many sources for determining their IoT product requirements, but
622 one key source of requirements is the customers' needs and goals. IoT product manufacturers
623 may be familiar with the concept of "requirements" as the set of attributes that various entities
624 within the IoT ecosystem impose upon the IoT product. Design requirements for IoT products,
625 including those for cybersecurity, are multi-faceted and can be imposed or implied from
626 different sources. For example, the IoT manufacturer's personnel skillset may create
627 requirements with respect to which parts of the IoT product could be developed "in-house" by
628 the IoT manufacturer's workers themselves and which parts need to be acquired as part of the
629 supply chain. Contractual obligations, business relationships between IoT ecosystem entities,
630 and other supply-chain dependencies can also create requirements for an IoT product. For
631 example, the IoT product manufacturer may have limitations on which cloud provider to use as
632 host of a backend IoT product component based on which providers the IoT product
633 manufacturer's parent company has pre-existing relationships with. Of all sources of
634 requirements, the customer will always be one member of the IoT product's ecosystem and will
635 also be an important source of cybersecurity requirements, as discussed in Section 2.

636   *Customers* are the individuals or organizations who purchase and
637   deploy an IoT product and will commonly act as administrators of the
638   product for cybersecurity purposes, making use of product
639   cybersecurity capabilities to help achieve their needs and goals. In
640   addition to customers, some IoT products may have other *users* who did
641   not purchase the equipment but nonetheless interact with the device or
642   other IoT product components and may have cybersecurity needs and
643   goals as well. Most customers are also users of the IoT products they
644   purchase, but not all IoT products have users in addition to the
645   customer. The rest of this publication will refer to customers since every
646   IoT product has a customer, but as discussed next, manufacturers
647   should consider *how* a product may be used, including whether there
648   may be users of the IoT product other than the customer.

649 Identifying the expected customers for an IoT product early in its design is vital for determining
650 which product cybersecurity capabilities the product should implement and how it should
651 implement them. For example, a large company might need an IoT product to integrate with its
652 log management servers, but a typical home customer would not. Manufacturers can answer
653 questions like the following:

654 1. **Who are the expected individuals to be customers or users for this product?** (e.g.,
655   musicians, small business owners, cyclists, police officers, chefs, home builders,
656   preschoolers, electrical engineers, seniors, students)

657 2. **What types of organizations are expected to acquire this product?** (e.g., individual home
658   users, small retail businesses, large hospitals, energy companies with solar farms,
659   educational institutions with buses)

660 Another early step in IoT product design is defining expected use cases for the product based
661 on the expected customers. To help define a use case, manufacturers can answer the following
662 questions, based on how they anticipate the product will be reasonably deployed and used:

663 1. **How will the product be used?** (e.g., for a single purpose or for multiple purposes;
664   embedded within another IoT product or not embedded, single user or customer or
665   multiple users; private or commercial use)

666 2. **Where geographically will the product be used?** (e.g., countries, jurisdictions within
667   countries)

668 3. **What physical environments will the product be used in?** (e.g., inside or outside; stationary
669   or moving; public or private; movable or immovable; extreme or specific physical and
670   weather conditions)

671 4. **What digital environments will the product be used in?** (e.g., unmanaged Wi-Fi networks;
672   managed enterprise or industrial networks)

673 5. **How long is the product expected to be used?** (e.g., a few hours; several years; two
674   decades)

675 6. **What IoT product components besides the IoT device will the product rely on to function?**
676   (e.g., a backend; companion application; or specialty networking/gateway hardware)

677 7. **What external dependencies on other systems will the product likely have?** (e.g., requires
678   use of a particular third-party IoT hub or can integrate with third-party management
679   applications)

680 8. **How might attackers misuse or compromise the product in the expected physical and
681   digital environments?** (i.e., potential pairings of threats and vulnerabilities, such as in a
682   threat model including consideration of network connections that may provide a path to
683   the internet that can be used as a vector of attack against other networks or devices)

684 9. **What kinds of data will the product create from its sensors or need to actuate on the
685   environment?** (e.g., will create video from a camera, will need location data for weather to
686   adjust thermostat)

10. **What other aspects of product use might be relevant to the product's cybersecurity risks?**
    (e.g., operational characteristics of the IoT device component that may have safety, privacy, or other implications for users)

3.3. Activity 2: Research Customer Cybersecurity Needs and Goals

Though a specific customer's cybersecurity needs and goals will be defined by a number of factors, cybersecurity needs and goals will be primarily driven by the cybersecurity risks they face. Manufacturers cannot completely understand all of their customers' risks because every customer, system, and IoT product faces unique risks based on many factors. However, manufacturers can consider the expected use cases for their IoT products, then make their IoT products at least minimally securable for these expected customers and use cases. *Minimally securable* means the IoT product has the product cybersecurity capabilities customers will likely need to mitigate some common cybersecurity risks, thus helping to at least partially achieve their goals and fulfill their needs. Customers also have a role in securing their IoT products and the systems that incorporate them, including following manufacturer set up instructions and using additional technical, physical, and procedural means (e.g., the use of a network firewall). The degree to which a customer may have a role will vary, but for most customers and use cases, product cybersecurity capabilities built into IoT products generally make risk mitigation easier and more effective for customers.

As Fig. 4 demonstrates, the cybersecurity connections between manufacturers and customers are important to keep in mind. Customers who buy and use IoT products are intending to connect those products to systems and networks, including the internet. As customers adopt these products, they will seek to secure them in order to meet their needs and goals which may or may not be articulated by the customer directly. IoT products that provide the product cybersecurity capabilities customers need or expect will be easier for customers to secure. Manufacturers can anticipate many customer cybersecurity needs and goals, especially those based on existing cybersecurity guidelines and requirements—for example, customers in a particular sector may be required by regulations to change all default passwords.
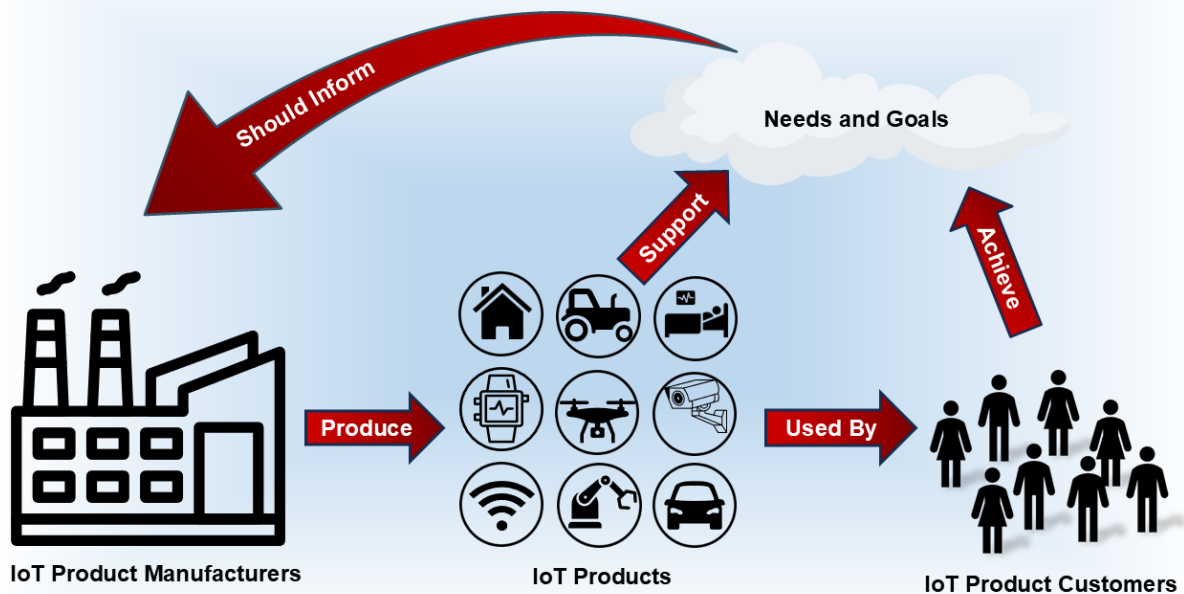
Figure 4: Cybersecurity connections between IoT product manufacturers and customers.

Cybersecurity risks for IoT products can be thought of in terms of two high-level risk mitigations. The first is safeguarding the cybersecurity of the product itself—to prevent the product from negatively impacting the customer or others through misuse or failing to provide expected functionality. The second is safeguarding the confidentiality, integrity, and availability of data (including personal information) collected by, stored on, processed by, or transmitted to or from the IoT product.

To gather information on customer needs and goals related to safeguarding the cybersecurity of the product and its data confidentiality, integrity, and availability, manufacturers can answer the following questions for each of the expected use cases:

1. **How will the IoT product interact with the physical world?** Some IoT products affect the physical world (or physical objects in the world), either directly through actuation or indirectly through measurement. In some cases operational requirements for performance, reliability, availability, resilience, and safety may be at odds with common cybersecurity practices. For example, many safety-critical products must continue to provide some or all functionality in the event of a cybersecurity incident, network issue, or other adverse condition.

2. **How will the IoT product need to be accessed, managed, and monitored by authorized people, processes, and other devices and products?** Considerations include:

   - The methods likely to be used by customers to manage the product are important. An IoT product could support integration with common enterprise systems (e.g., asset management, vulnerability management, log management) to give customers greater control over and visibility into the product. For an IoT product expected to

be used in home environments only, this capability would not be relevant; instead customers would expect a user-friendly way to manage their products, or even want the manufacturer to perform all management on their behalf (e.g., install patches automatically). IoT products used by a small business might also be managed by a third party on behalf of the business.

- Making a product highly configurable is generally more desirable in organizational environments and less so in home customer settings. A home customer is less likely to understand the significance of granular cybersecurity configuration settings and thus may misconfigure a product, weakening its security and increasing the likelihood of a compromise. Some home customers are also unlikely to want to change configuration settings after initial deployment. However, some configuration settings, such as enabling or disabling clock synchronization services for the product and choosing a time server to use for clock synchronization, may be desired by many customers, including industrial, enterprise, and home customers. Product configuration might be entirely omitted in the rare cases where the product does not need to be provisioned or customized in any way during or after deployment.

- How accessible the product is, either logically or physically, could impact the attack surface. An IoT food vending machine in a public place, which is internet connected so suppliers can track inventory and machine status, is highly accessible. Vending machine users would not be required to authenticate themselves in order to insert money and purchase a snack. Authorized employees of the vending machine owner, though, will likely have a method to authenticate to physically restock the machine and change item prices and, potentially, remotely change the prices as well. However, the vending machine would also be highly susceptible to physical attack, so any authentication interface and physical ports that can be used by other digital technology (e.g., USB, ethernet) should not be publicly accessible.

- Whether the IoT device or other IoT product components should have an open application programming interface (API) to support third-party integration, support, or development. Access to an API should be carefully considered and managed as a logical interface, since it can offer significant access and functionality to authorized entities.

- The benefits of allowing customers to disable product cybersecurity capabilities that may negatively impact operations. An example is a capability intended to deter brute force password attacks, such as locking out an account after too many failed authentication attempts. Such a capability can inadvertently cause a denial of service for the person or other computing device attempting to authenticate. In safety-critical environments such as healthcare delivery, such disruptions to access may not be acceptable because of the danger they would pose to human safety. Customers may need flexibility in configuring such features or installing compensating controls.

- Determining expectations about product lifespan and how that may impact feasibility of product cybersecurity capabilities through the expected lifespan of the product will help support cybersecurity throughout the product's lifespan. Some product cybersecurity capabilities, such as software updates, will require ongoing development and effort to provide the intended cybersecurity benefits, and so manufacturers need to consider how long they can realistically support such a capability. Additionally, some IoT products may have non-IT based features that can outlive the anticipated cybersecurity or functionality lifespan for IT components of the product, which can complicate cybersecurity later in the lifecycle of the product.

3. **What are the known cybersecurity requirements for the IoT product?** Manufacturers can identify known requirements in their use cases, such as sector-specific cybersecurity regulations, country-specific laws, contractual obligations, or customer expectations and conventions so they can be mindful of those requirements during product cybersecurity capability identification. For example, some customers may have mandates to use multi-factor authentication or zero-trust authentication for all devices.

4. **How might the IoT product's use of product cybersecurity capabilities be interfered with by the IoT product's operational or environmental characteristics?** For example, some IoT products, such as connected medical equipment, may provide critical non-IT-based functionality to customers, so customers may need the IoT product's device functions to continue operating even during a degraded cybersecurity state or when IT-related functionality (e.g., an internet connection) is unavailable.

5. **What will be the nature of the IoT product's data?** There is a great deal of variability in data stored by IoT devices and other IoT product components; some devices do not store any data, while others store data that could cause significant harm if accessed or modified by unauthorized entities. Conversely, most backends store significant IoT product data, but some merely pass data to other IoT product components. Understanding the expected data on all IoT product components for the anticipated use cases can help manufacturers identify which product cybersecurity capabilities (e.g., data encryption, device and user authentication, data validation, access control, backup/restore) may be needed to protect data.

6. **What degree of trust in the IoT product may customers need?** Customers may expect certain cybersecurity capabilities and implementations of those capabilities that provide specific assurances about the cybersecurity of the product and data. For example, in some contexts, additional trust that data is protected could be achieved by adding protection of data in use within the device. This would go beyond the usual goals of data protection (e.g., protecting data at rest and in transit).

7. **What complexities will be introduced by the IoT product interacting with other devices, systems, and environments?** For example, complexity can be driven by new uses of IoT and IoT products; new combinations of those products with each other and conventional IT; and increasing interconnections among devices and systems. These complexities could mean new functionality that will be connected via networking technologies to systems that do not appropriately mitigate these risks, which may have human-safety or privacy impacts. An IoT

820   product that can stream images from inside the home (e.g., a smart baby monitor) or that
821   can alter the environment to the point of danger (e.g., a smart oven), might require
822   safeguards not usually considered for conventional IT. IoT can also introduce complexities
823   related to scale of deployment, which could make ongoing management and support of
824   products difficult.

825   By answering these questions, manufacturers can identify for each of the anticipated use cases
826   the reasonable threats to the IoT product, how the IoT product may be vulnerable to the
827   threats, and what could be the resulting risks to customers and operational environments.
828   Reasonable threats to consider include those that may harm customers or other IoT product
829   users and bystanders, harm the manufacturer, or harm third party individuals and organizations
830   inside and outside the IoT product's ecosystem. Threats that can impact these entities will
831   include those to the operations of the IoT device, other IoT product components, as well as
832   threats to the IoT product's data and resources (e.g., its network connection to act as part of a
833   DDoS attack).

834   Even with an understanding of reasonable threats, manufacturers may not be able to conduct a
835   complete assessment of risk since many elements of the customers' operating environment
836   may be unknown. However, manufacturers can perform an *initial assessment of risk* for the
837   expected use cases using documented assumptions that will guide the identification of product
838   cybersecurity capabilities.

839 | An initial risk assessment is distinct from a risk assessment in that an
840 | initial risk assessment is performed without full knowledge of the
841 | deployment environment and cybersecurity expectations. Like with all
842 | risk assessments, performance of an initial risk assessment requires
843 | understanding of threats, vulnerabilities, etc., but focuses on the
844 | threats, vulnerabilities, etc. that can be assumed and expected based on
845 | the IoT product's design, components, etc., as well as characteristics
846 | ascertainable about the customer, such as their cybersecurity
847 | expectations. Sources of information that can be helpful in performing
848 | an initial risk assessment include, but are not limited to, guidelines from
849 | NIST or other organizations, national and international voluntary
850 | consensus standards, national and international regulations, and
851 | industry best practices.

852   As Fig. 5 conceptually depicts, IoT product manufacturers can use a variety of sources to gather
853   the information they need to answer these questions and others. In some instances, expected
854   customers and use cases will point to existing laws, regulations, or voluntary cybersecurity or
855   operational guidelines. For example, IoT products intended to be used by the federal
856   government would be secured using controls derived from system cybersecurity guidelines that
857   are required for federal agencies (e.g., NIST SP 800-53 [5], Cybersecurity Framework [8], NIST
858   SPs 800-213 [17] and 800-213A), which in some cases identify or imply specific product
859   cybersecurity capabilities that an agency would need to support controls used in their system.
860   For some use cases, guidance may go beyond cybersecurity risks but will still have direct or

861   indirect implications for cybersecurity, such as devices in the medical sector needing to comply
862   with Food and Drug Administration (FDA) regulations and the Health Insurance Portability and
863   Accountability Act (HIPAA). It is possible that in order to meet FDA recommendations and
864   HIPAA requirements, an IoT product may need strict data confidentiality, integrity, and/or
865   availability protections well beyond what is included in an average IoT product. By
866   understanding these regulations in the context of the expected use cases, manufacturers can
867   determine how to best support their customers' needs and goals. Many industrial sectors will
868   also have consensus and/or voluntary guidelines (e.g., frameworks, baselines, and best
869   practices) that should be followed by their stakeholders. In the healthcare context, one
870   example of a voluntary consensus standard is *Health software and health IT systems safety,*
871   *effectiveness and security Part 5-1: Security — Activities in the product life cycle*, IEC 810015-1 ,
872   while for industrial control system devices, manufacturers could look to *Security for industrial*
873   *automation and control systems - Part 4-1: Secure product development lifecycle requirements*,
874   ISA/IEC 62443-4-1 . Increasingly, geographic regions may have voluntary or mandatory IoT
875   product cybersecurity programs, such as the Cyber Security Agency of Singapore's
876   Cybersecurity Labelling Scheme or the European Union's Cyber Resilience Act.

877
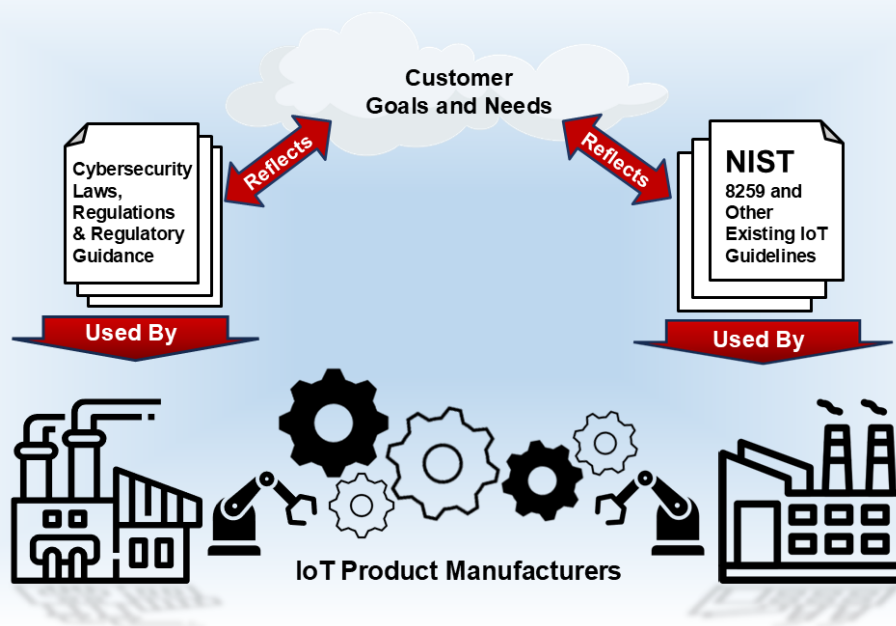
878   **Figure 5: . Customer cybersecurity needs and goals reflected in and informed by many applicable regulations and**
879   **other documents.**

880   For some customers or sectors, such explicit documents may not be readily available or usable
881   (e.g., due to high variability in needs and goals for customers within a sector). For products
882   intended to be used by these customers, ascertaining their needs and goals may require use of
883   other forms of information, such as gathering information directly from customers or
884   conducting secondary research.

885 **3.4. Activity 3: Determine Appropriate Means to Support Customer Needs and Goals in the**
886   **Context of the IoT Product**

887 After researching the cybersecurity needs and goals for the IoT product's expected customers
888 and use cases, manufacturers can determine how to address those needs and goals in order to
889 help customers mitigate cybersecurity risks. For this activity, manufacturers should consider
890 other factors related to the IoT product and its ecosystem in addition to customer cybersecurity
891 needs and goals, since these other factors will have impacts on which means are appropriate
892 and applicable for the IoT product.

893
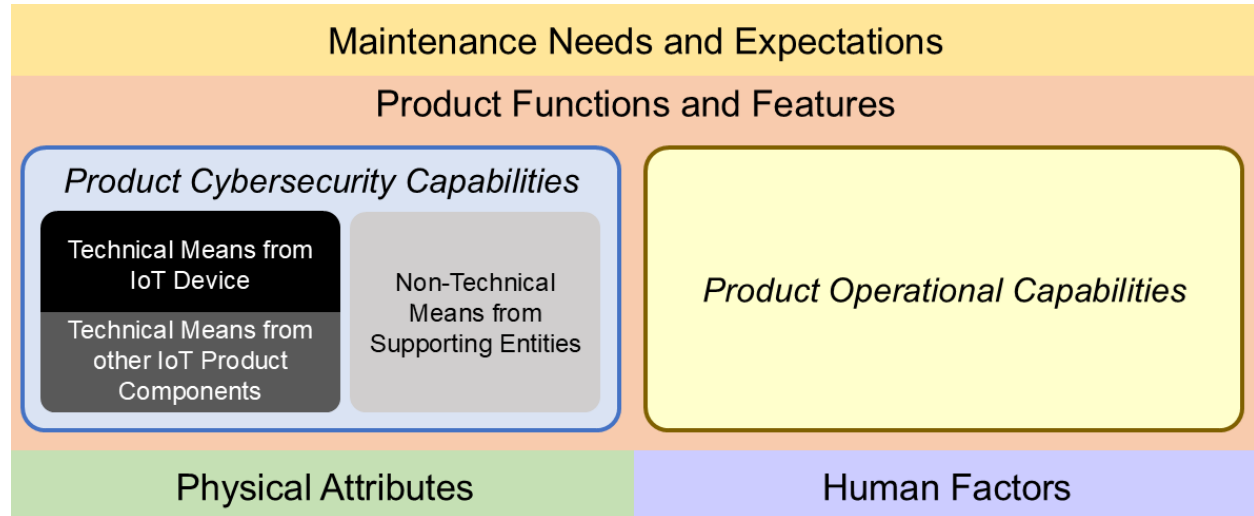
894 **Figure 6: How other factors can build up to include, but not be limited to, the product cybersecurity capabilities**
895 **composed of technical and non-technical means.**

896 Fig. 6 shows how factors related to IoT products stack such that higher factors are defined, in
897 part, by lower factors. The operational and cybersecurity capabilities will depend on the
898 physical attributes and human factors of the IoT product, balancing product features and
899 functions based on these factors. For example, a healthcare product that lacks usable
900 authentication capabilities for the clinical environment may interfere with human factors like
901 patient care. Based on product features and functions, maintenance needs and related
902 expectations can be identified.

903 Note, Fig. 6 is focused on those factors specifically related to the IoT product, and so customer
904 needs and goals are not captured directly. Rather all factors depicted would be tailored to align
905 with and support customer needs and goals. Means will be used to satisfy each of these factors,
906 but this publication is primarily concerned with product cybersecurity capabilities and the
907 technical and non-technical means used to satisfy those capabilities. As discussed in Section
908 2.6, there is an important relationship between cybersecurity needs and goals, product
909 cybersecurity capabilities, and technical and non-technical means.

910 Therefore, IoT product manufacturers can use the understanding gained from the prior activity
911 about their customers' needs and goals--including those around cybersecurity--to determine
912 how they and their IoT product should support cybersecurity. IoT product manufacturers can
913 start with identifying technical and non-technical means that can support customers' needs and

914 goals. For each cybersecurity need or goal, the manufacturer can answer this question to help
915 think about how the need or goal could be supported: **which one or more of the following is a**
916 **suitable means (or combination of means) to achieve the need or goal?**

917 1. The IoT device can provide the technical means through its device cybersecurity capabilities
918   (for example, by using device cybersecurity capabilities built into the device's operating
919   system).

920 2. Another IoT product component can provide the technical means on behalf of the IoT
921   device. This may include other systems and services that may or may not be acting on
922   behalf of the manufacturer providing the technical means (e.g., a cloud-based service that
923   securely stores data for each IoT product, internet service providers and other
924   infrastructure providers).

925 3. In addition to and in support of technical means, non-technical means (e.g., communication
926   of lifespan and support expectations, disclosure of flaw remediation plans) can also be
927   provided by manufacturers or other organizations (i.e., supporting entities) and services
928   acting on behalf of the manufacturer.

929 4. The customer can select and implement other technical and non-technical means for
930   mitigating cybersecurity risks. The customer can also choose to respond to cybersecurity
931   risks in other ways, including accepting or transferring the risk. For example, an IoT product
932   may be intended for use in a customer facility with stringent physical security controls in
933   place and thus may not support multi-factor authentication for access control to the IoT
934   device component.

935 Note that there is not necessarily a one-to-one correspondence between needs or goals and
936 means; for example, it may take multiple technical means to achieve a goal, and a single
937 technical means may help address multiple goals. Additionally, not all needs and goals can or
938 need to be addressed using only technical means, and some technical means themselves may
939 require additional non-technical means for initial and on-going securability (e.g., knowledge of
940 which product cybersecurity capabilities are available, ability to gather and apply software
941 updates). As noted in the list, some means may be selected and implemented *by the customer*,
942 which will be outside the scope of a manufacturer's control, but other means should be
943 implemented as product cybersecurity capabilities (i.e., items 1-3 in the list above).

944 Not all means will be appropriate or applicable for the IoT product. Customers may have needs
945 and goals for cybersecurity that require means which cannot be supported by the IoT product
946 due to limitations such as resource constraints, form-factor constraints, etc. For example, a
947 customer may have rigorous data protection needs and goals, but the IoT device component of
948 the IoT product may not have sufficient energy resources to implement strong encryption.
949 Contractual, regulatory, and legal obligations for the manufacturer and their suppliers may also
950 dictate or limit appropriate and applicable means. Manufacturers should consider all sources
951 for and limitations on appropriate means when determining those that their customers will
952 need and expect to support their needs and goals, such as:

953   •   The manufacturer's attributes and resources since supply chains, design
954   methodologies, cybersecurity governance structures, and other business and
955   organization factors will vary.

956   •   Ecosystem obligations like applicable standards, laws, and regulations or contractual
957   obligations the manufacturer may have with other entities.

958   •   Physical product considerations such as size, shape, and weight which can limit or
959   otherwise influence the selection of appropriate and applicable means for
960   cybersecurity.

961   •   IoT product lifecycle and maintenance expectations may impact the selection of means,
962   especially those that require on-going support through the lifecycle or frequent
963   maintenance.

964 Fig. 7 illustrates how these factors collide to shape an IoT product's appropriate and applicable
965 technical and non-technical means for cybersecurity.

966
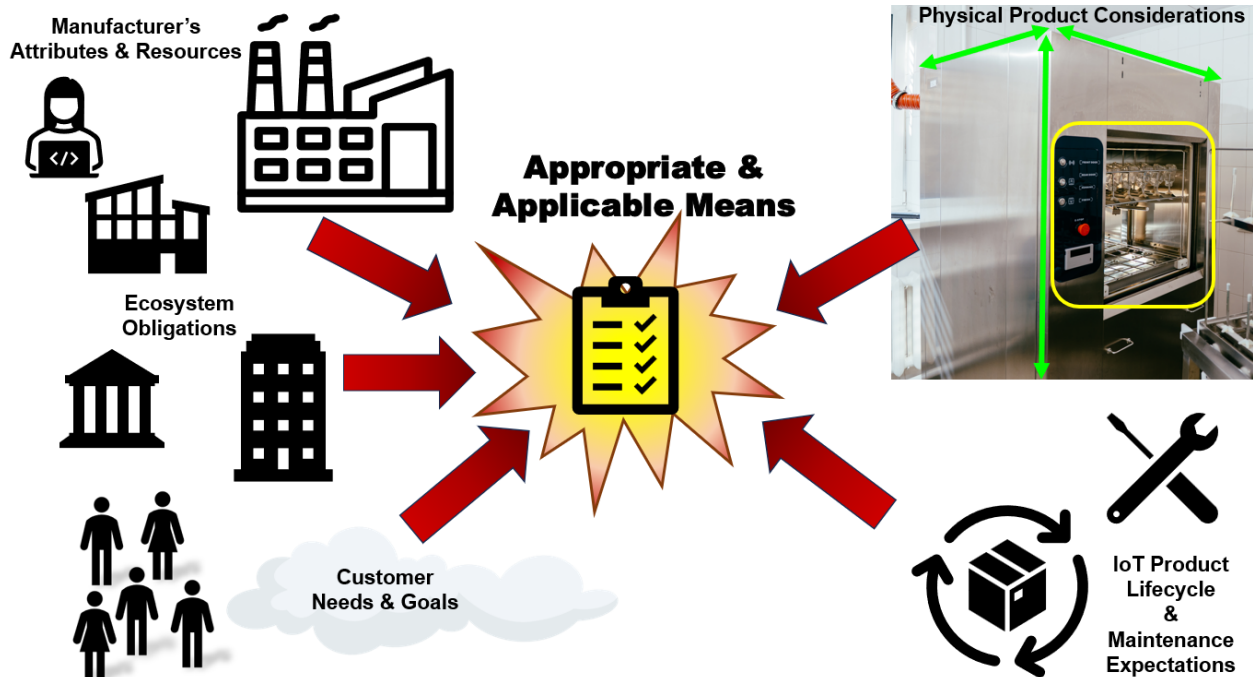
967   **Fig. 7. Various factors combine to influence appropriate and applicable means for cybersecurity.**

968 IoT manufacturers could use an understanding of means to document and express
969 cybersecurity support they aim to provide for their IoT product. Organizing technical and non-
970 technical means and using them to define product cybersecurity capabilities can enable a
971 broader view of cybersecurity throughout the IoT product's lifecycle and easier communication
972 about cybersecurity features with various ecosystem entities.

3.5. Activity 4: Define IoT Product Cybersecurity Capabilities Based on Appropriate Means

An understanding of appropriate means to support customer needs and goals is prerequisite to determining which of those means should guide different kinds of IoT product cybersecurity capabilities. In addition to identifying suitable means to define IoT product cybersecurity capabilities for addressing each cybersecurity need and goal, manufacturers can also answer this question related to the technical means provided through their IoT product: **how robustly must each technical means related to product cybersecurity capabilities be implemented in order to achieve the cybersecurity need or goal?** Robustness of technical means refers to the overall strength of the means' implementations and is related to the trust a customer may expect to have in their IoT product. If a product is expected to be more trusted by customers, particularly to remain in a secure state and stay outside the control or access of unauthorized entities, then it is likely that technical means implemented in that product will have to be more robust. Robust product cybersecurity capabilities will consider not only appropriate security means for the situation, but also how resilient those means are to interference, manipulation, and direct attack, how reliably they operate, how usable they are, etc.

Here are some examples of potential robustness considerations:

- Whether the means needs to be implemented in hardware and/or software (e.g., a cryptographic hardware component paired with software to use the hardware's functionality)

- Which data needs to be protected, what types of protection each instance of data needs (i.e., confidentiality, integrity, availability), and how strong that protection needs to be

- How strongly a human or an entity's identity needs to be authenticated (e.g., PIN, password, passphrase, two-factor authentication, passkey) before being granted access to a system, or another device, process, or service

- Whether data received by or inputted into any product component needs to be validated (e.g., to confirm the legitimacy of an update, to restrict the ability of malformed data to bypass access controls)

- How readily software updates can be reverted if a problem occurs (e.g., a rollback capability to a secure state, an anti-rollback capability for specific types of security updates)

Ultimately, manufacturers can aggregate the technical means identified for all the needs and goals to determine the product cybersecurity capabilities expected customers will need. Not all identified technical means will be part of a product cybersecurity capability, but some will, and the rest of the means may need support and lack of interference from product cybersecurity capabilities. To determine which technical means may need to be part of product cybersecurity capabilities, manufacturers can answer the following question: **which technical means must be provided by the IoT device itself, other IoT product components, other systems and services acting on behalf of the manufacturer, and the customer's other cybersecurity controls?**

Product cybersecurity capabilities that are implemented by technical means in an IoT device specifically (i.e., implemented by the IoT device's hardware and software) are called device cybersecurity capabilities. Identifying any device cybersecurity capabilities that the device itself

1013   needs to provide should happen as early as feasible in the product design processes so the
1014   capabilities can be considered when selecting or designing IoT product hardware and software.
1015   To provide manufacturers a starting point in identifying the necessary device cybersecurity
1016   capabilities for their IoT devices, a companion publication the IoT Device Cybersecurity
1017   Capability Core Baseline, NISTIR 8259A defines a device cybersecurity capability core baseline,[4]
1018   which is a set of device capabilities generally needed to support common cybersecurity controls
1019   that protect the customer's devices and device data, systems, and ecosystems. The device
1020   cybersecurity capability core baseline has been derived from common cybersecurity risk
1021   management approaches. The core baseline is just one set of product cybersecurity capabilities
1022   that may be needed in an IoT product, and manufacturers should consult other sources to
1023   identify appropriate product cybersecurity capabilities for expected customers and use cases.

1024   Other IoT product components, as well as other systems and services acting on behalf of the
1025   manufacturer, will likely need to contribute to product cybersecurity capabilities. The technical
1026   means by which IoT product components and other systems and services will contribute to
1027   product cybersecurity capabilities will vary, and who implements and manages those means
1028   may also vary. Consider an IoT product comprised of an IoT device and a backend. Some
1029   product cybersecurity capabilities (e.g., data protection) would likely be implemented similarly
1030   by the IoT device and backend, but not always exactly the same. Protecting data at rest on the
1031   IoT device or on the backend would use similar methods, likely utilizing encryption modules. On
1032   the other hand, protecting the data stored on each component when "resetting" the product
1033   may be implemented differently; while all data would likely be deleted from the IoT device, the
1034   data may be preserved on the backend for the customer to access as an archive.

1035   To identify how each IoT product component should support product cybersecurity capabilities,
1036   manufacturers can follow a process of linking cybersecurity mitigations, needs, and goals with
1037   specific IoT product components and the product cybersecurity capabilities they support. This
1038   process was used to define the device cybersecurity capability core baseline in NISTIR 8259A.
1039   High-level cybersecurity mitigations, needs, and goals common across many customers were
1040   identified to determine the common device cybersecurity capabilities needed by many of these
1041   customers from the IoT device component of IoT products.

1042   Additional baselines of IoT product cybersecurity capabilities may exist from NIST or other
1043   organizations, some of which may be designed to address the needs of particular customer
1044   groups, industrial sectors, use cases, etc. For example, NIST has published *Profile of the IoT Core*
1045   *Baseline for Consumer IoT Products*, NISTIR 8425 [21] and *IoT Device Cybersecurity Guidance for*
1046   *the Federal Government: IoT Device Cybersecurity Requirement Catalog*, SP 800-213A [18].
1047   These resources can help manufacturers identify necessary product and device cybersecurity
1048   capabilities for the context in which their IoT device will be used.

---

[4] 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 NIST Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations [5] to help federal agencies meet their obligations under the Federal Information Security Modernization Act (FISMA) and other federal policies. In that context, the low-, moderate-, and high-impact control baselines apply to an information system, which may include multiple components, including devices. In this publication, "baseline" is used in the generic sense to refer to a set of foundational requirements or recommendations that would apply to individual IoT devices intended to be used as components within systems.

1049 Since product cybersecurity capabilities will be shaped by the context of the customer and use
1050 case, different IoT products will need different *sets* of product cybersecurity capabilities.
1051 Though useful as a starting point, the high level of the device cybersecurity capability core
1052 baseline means that it will need to be profiled for specific IoT products based on the needs and
1053 goals of the expected use case. Product cybersecurity capabilities drawn from the core baseline
1054 or other high-level sources can be profiled and built upon in a variety of ways. New or more
1055 complex capabilities may be required in a product. High-level product cybersecurity capabilities
1056 can be expanded and adapted in ways that better align with what specific customers need or
1057 prefer (e.g., product cybersecurity capabilities adapted for the federal government [18]).

3.6. Activity 5: Plan for Adequate Support of Customer Needs and Goals

1059 It is important for manufacturers to consider how to support customers' needs and goals
1060 beyond the selection of specific product cybersecurity capabilities and their implementations.
1061 Manufacturers should also consider how to provision computing resources to support product
1062 cybersecurity capabilities and what actions may be needed to support cybersecurity needs and
1063 goals.

1064 First, manufacturers can help make their IoT products more securable by appropriately
1065 provisioning the products' IoT device hardware resources (e.g., processing, memory, storage,
1066 network technology, power) and software resources. IoT product manufacturers should
1067 consider that decisions they make in the design of their products, such as selection of hardware
1068 and software, can have impacts on securability. For example, software-based encryption is
1069 processing-intensive, and a device with limited processing and no hardware-based encryption
1070 might not be able to provide what customers need. Another example is that some devices
1071 cannot support the use of an operating system or Internet Protocol (IP) networks. IoT product
1072 manufacturers should make decisions to support cybersecurity not just today, but for all stages
1073 of the IoT product's lifecycle. When designing or selecting device hardware and software
1074 resources, manufacturers can answer the following questions for the expected customers and
1075 use cases to help identify provisioning needs and potential issues:

1076 1. **Considering expected terms of support and lifespan, what potential future use needs to**
1077   **be taken into account?** For example, if a product has a 10-year lifespan, it may be necessary
1078   to update the encryption algorithm or key length the product uses during that time, and the
1079   new algorithm or key length may require more processing resources than is currently
1080   provided. Consider how the product can support cybersecurity needs and goals for the
1081   product's lifespan, including "future proofing" of the product cybersecurity capabilities and
1082   their implementations. As an IoT product moves deeper into its lifespan, the ability for
1083   customers to determine the support status for products is important to making products
1084   securable.

1085 2. **Should an established IoT platform be used instead of acquiring and integrating individual**
1086   **hardware and software components?** An *IoT platform* is a piece of hardware or supporting
1087   software upon which a new IoT product can be created. IoT platforms may have some IoT
1088   product components or capabilities already installed and configured for a manufacturer's
1089   use. An IoT platform might also offer various configuration capabilities, third-party services

1090   or applications, or a software development kit (SDK). Manufacturers can choose a
1091   sufficiently resourced and adequately secure IoT platform to reduce some or all of the
1092   cybersecurity risks associated with designing hardware, installing and configuring an
1093   operating system, creating new cloud-based services, writing IoT product component
1094   applications and mobile apps from scratch, and performing other tasks that are error-prone.

1095   3. **Should any of the product's, especially the device's, cybersecurity capabilities be**
1096   **hardware-based?** An example is having a hardware root of trust that provides trusted
1097   storage for cryptographic keys and enables performing a secure boot and confirming the IoT
1098   product and device authenticity. Further, manufacturers should consider whether those
1099   hardware-based capabilities will be updatable, such as to facilitate a move to post-quantum
1100   cryptography when possible. For example, in some cases, customers will need an
1101   immutable hardware root of trust and never want updates or changes to that functionality,
1102   but such limitations could be detrimental to ongoing securability for other customers.

1103   4. **Does the hardware or software (including the operating system) include unneeded**
1104   **product capabilities with cybersecurity implications? If so, can they be disabled to prevent**
1105   **misuse and exploitation?** For example, an IoT device may have local interfaces on its
1106   external housing that are essential for some current, or future expected, use cases. But if
1107   the device may be deployed in public areas, those interfaces would be exposed to possible
1108   attack. Possible approaches to this issue include offering a tamper-resistant enclosure to
1109   prevent physical access to the interfaces or providing a configuration option that logically
1110   disables the interfaces.

1111   Beyond the IoT device hardware and software resources, manufacturers can improve
1112   securability of IoT products by appropriately implementing product cybersecurity capabilities
1113   across all IoT product components. For example, data stored in backends, companion
1114   applications, or specialty networking/gateway hardware should be protected using the same or
1115   similar means as in the IoT device. When designing or selecting hardware and software
1116   resources for IoT product components other than IoT devices, manufacturers can answer the
1117   following questions for the expected customers and use cases to help identify provisioning
1118   needs and potential issues:

1119   1. **Which product cybersecurity capabilities are relevant to each IoT product component?**
1120   Manufacturers often design IoT products leveraging multiple IoT product components in
1121   ways that allow each component developer to specialize in actions for which they are best
1122   suited. For example, backends generally have near limitless storage and substantial
1123   processing capabilities, whereas companion applications have the benefit of access to the
1124   customer and mature, standardized interface capabilities. How an IoT product component
1125   fits into the IoT product's operations can impact the threats and risks that particular IoT
1126   product component faces and how those risks might be mitigated.

1127   2. **How can each relevant product cybersecurity capability be appropriately implemented for**
1128   **each IoT product component?** For example, a backend is generally inaccessible to
1129   customers; customer-facing product cybersecurity capabilities (e.g., asset identification for
1130   use by the customer) may be irrelevant. Other product cybersecurity capabilities (e.g.,
1131   software update capabilities for companion applications) may be supported differently,

1132   taking advantage of update capabilities provided by the operating system or other platform
1133   they run on. Still other product cybersecurity capabilities (e.g., protection of data at rest and
1134   in transit) may be implemented similarly across all IoT product components.

1135   3. **How can cybersecurity be supported within the IoT product boundary?** It is important to
1136   consider that an IoT product comprised of multiple IoT product components is a system,
1137   and cybersecurity protections within the boundary of the IoT product can utilize system
1138   cybersecurity techniques even if their customers do not expect them or use them. For
1139   example, cybersecurity within the IoT product boundary could be supported by
1140   implementation of a Zero-Trust Architecture.

1141   4. **How much control and cybersecurity responsibility will the customers, manufacturer, or**
1142   **other entities have over each IoT product component?** Cybersecurity in the context of IoT
1143   products will require some amount of coordination between manufacturers and customers
1144   and may involve other entities (e.g., installers, integrators). Manufacturers should consider
1145   how the IoT product can best support each of these entities throughout the product's
1146   lifecycle. This support will vary depending on how much control each entity has over
1147   cybersecurity and how much cybersecurity responsibility each entity has. Refer to Section 3
1148   of this document for a discussion of these considerations.

1149   5. **How can necessary cybersecurity support be coordinated for all IoT product components,**
1150   **potentially across multiple entities?** Coordination between entities can take many forms.
1151   Expected technical product cybersecurity capabilities being present in equipment affords
1152   securability and allows entities to use the product securely. Sometimes coordination
1153   requires non-technical interactions, particularly if visibility into technology or organizations
1154   is limited. For example, backends can be hosted by third-parties that the manufacturer does
1155   not have insight into, necessitating the setting and enforcement of cybersecurity
1156   expectations through means such as business-to-business dialogue and contracts. For IoT
1157   products generally, there will be required interactions between manufacturers and
1158   customers. For example, since a manufacturer cannot anticipate all potential customers and
1159   users, they may rely on non-technical means such as disclaimers and warning messages to
1160   communicate key cybersecurity considerations in a way accessible to as many potential
1161   customers and users as possible. Even for customers and users that the manufacturer can
1162   anticipate, the complexities of deployment, installation, and use of IoT products may
1163   require non-technical cybersecurity support such as detailed lists of answers to frequently
1164   asked questions or text and video tutorials guiding customers and users in securely using
1165   the IoT product.

1166 Manufacturers should consider which secure development practices[5] and other non-technical
1167 supporting capabilities are most appropriate in planning how to adequately support customer
1168 needs and goals. Manufacturers can answer questions like the following based on expected

---

[5] IoT manufacturers interested in more information on secure software development practices can consult the NIST white paper Mitigating the
Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF) [18], which highlights selected practices for
secure software development. Each of these practices is widely recommended by existing secure software development publications, and the
white paper provides references from nearly 20 of these publications.

customers and use cases to help identify additional secure development practices to adopt in order to improve IoT product cybersecurity:

1. **How is IoT product code protected from unauthorized access and tampering?** (e.g., well-secured code repository, version control features, code signing)

2. **How can customers verify hardware or software integrity for the IoT device or other IoT product components?** (e.g., hardware root of trust, code signature validation, cryptographic hash comparison)

3. **What verification is done to confirm that the security of third-party software used within the IoT product meets the customers' needs?** (e.g., check for known vulnerabilities that are not yet fixed, review or analyze human-readable code, test executable code)

4. **What measures are taken to minimize the vulnerabilities in released IoT product software?** (e.g., follow secure coding practices, perform robust input validation, review and analyze human-readable code, test executable code, configure software to have secure settings by default, check code against known vulnerability databases)

5. **What measures are taken to accept reports of possible IoT product software vulnerabilities and respond to them?** (e.g., bug-bounty programs, vulnerability response and disclosure program, vulnerability database monitoring, threat intelligence service use, development and distribution of software updates)

6. **What processes are in place to assess and prioritize the remediation of all vulnerabilities in IoT product software?** (e.g., estimate remediation effort, estimate potential impact of exploitation, estimate attacker resources needed to weaponize the vulnerability)

7. **What cybersecurity conforming testing or labelling could potential customers look for in IoT products or IoT product components?** (e.g., United States Cyber Trust Mark for home IoT products, Cloud Security Alliance STAR for backends)

8. **Which cybersecurity risks were considered in development of the IoT product, what actions, controls, etc. are expected from customers, and how can expectations be effectively communicated?** (e.g., information in a manual explaining the expected integration of an IoT product into an asset management system that securely on-boards and inventories all end-points automatically)

9. **Are there aspects of the IoT product that have their own unique risk considerations and related frameworks or tools?** (e.g., machine learning, automated decision-making, and other forms of artificial intelligence that could be informed by the NIST AI Risk Management Framework [22], collection and processing of personal data that could be informed by the NIST Privacy Framework [23], use of digital identities that could be informed by *Digital Identity Guidelines*, NIST SP 800-63 Rev. 4 [24])

1204 **4. Manufacturer Activities Impacting the IoT Product Post-Market Phase**

1205 Manufacturers of IoT products will at some point market and sell their product, which will put it
1206 in the hands of customers and initiate the manufacturing post-market phase. Even in this
1207 phase, manufacturers continue to have a role in supporting IoT products and the customers'
1208 cybersecurity needs and goals. For example, manufacturers may have to respond to
1209 vulnerability reports and provide critical updates. These foundational cybersecurity activities
1210 may benefit customers and their ability to secure products throughout their life. An often-
1211 overlooked aspect of both marketing and the post-market phase is communication related to
1212 cybersecurity. Many customers will benefit from manufacturers clearly communicating about
1213 the cybersecurity of their products. This section discusses ongoing actions performed by the
1214 manufacturer that improve securability, making it easier for customers to understand product
1215 cybersecurity and how the IoT products meet their cybersecurity needs and goals.

1216 | The previous sections discussed how manufacturers can identify
1217 | technical or non-technical means customers and users of their IoT
1218 | products may need for cybersecurity, including *product cybersecurity*
1219 | *capabilities.* This section is intended to help manufacturers support the
1220 | cybersecurity of a product through the post-market phase, most
1221 | notably through highlighting the best approaches for communication
1222 | with customers and users about cybersecurity related to their IoT
1223 | product. Some considerations may discuss additional product
1224 | cybersecurity capabilities and/or other actions or services the
1225 | manufacturer can implement that may be appropriate for some
1226 | customers and should be communicated to them.

1227 Planning for these activities, though likely not fully completed until an IoT product is in the
1228 post-market phase, is best performed during pre-market activities, such as those discussed in
1229 Section 3. Though Activities 0 through 5 may help inform planning and execution of the
1230 activities presented in this section, they are not considered a prerequisite. This allows aspects
1231 of the planning for Activities 6, 7, and 8 to happen in parallel with other pre-market activities.
1232 The considerations mentioned within these activities may not apply to all customers or
1233 manufacturers, but many will find these considerations to be vital.

1234 **4.1. Activity 6: On-Going Support of Product Cybersecurity through-out the Lifecycle and**
1235 **through End-of-Life**

1236 On-going securability of IoT products through the post-market phase will often require actions
1237 by customers, manufacturers, and other entities. Some cybersecurity mitigations, such as
1238 vulnerability remediation via software updates, are critical post-market means that customers
1239 may rely on to maintain the security of their products and the systems to which they are
1240 connected. Activity 5 discussed planning in the pre-market phase that would be executed upon
1241 here in the post-market phase. Manufacturers can answer the following questions to
1242 understand what actions they or other supporting entities may need to take in the post-market
1243 phase to support product cybersecurity:

1244 1. **Which product cybersecurity capabilities *require* post-market cybersecurity support?**
1245   Product cybersecurity capabilities may need to be updated over time. For example, digital
1246   asset identifiers may be upgraded to accommodate more unique values as a product base
1247   grows. Software updates will also be deployed post-market, which will be critical to keeping
1248   IoT products in service longer and minimizing open vulnerabilities across the internet.

1249 2. **Which product cybersecurity capabilities *enable* post-market cybersecurity support?** Some
1250   product cybersecurity capabilities may be important to enabling post-market cybersecurity
1251   support. Considering the prior example of updating a digital asset identifier, software
1252   update capabilities could be used to achieve these updates. Non-technical cybersecurity
1253   capabilities (e.g., Information and Query Reception and Information Dissemination
1254   documented in NIST IR 8259B [11]) are critical to facilitating post-market cybersecurity
1255   support.

1256 3. **How can all ecosystem entities be proactive in identifying and mitigating emerging
1257   cybersecurity threats and risks?** During the post-market phase, manufacturers are not
1258   alone in ensuring the cybersecurity of the IoT product. They may have a role in ensuring on-
1259   going securability of the product, but so may other ecosystem entities. There may be
1260   various actions participants in this ecosystem can take to ensure threats are visible and risks
1261   are mitigated, for example:

1262   • IoT product manufacturers can prioritize actions on vulnerability and bug reports from
1263   the public by making software updates to remediate the issues.

1264   • Integrators can maintain awareness of known issues with IoT products they have
1265   installed for customers and work with customers to minimize the risks.

1266   • Customers can seek support information for their IoT products, ensure the most up-to-
1267   date software is installed, and plot next steps if products are out of their support
1268   period and are no longer receiving updates.

1269 4. **As cybersecurity and other digital support for the IoT product ends, what actions will the
1270   manufacturer take to ensure the products remain securable?** IoT products may remain in
1271   service much longer than software or other digital components are supported or state-of-
1272   the-art. Unsupported or deprecated digital equipment used in the field is sometimes called
1273   "legacy." Though legacy IT equipment is an issue for some sectors, legacy IoT products are
1274   relatively common, especially for industrial applications. Unmanaged environments, (e.g.,
1275   homes and small businesses) can also accumulate legacy IoT products. Use of legacy
1276   products is not natively a cybersecurity issue, but legacy products have significantly higher
1277   likelihood of the presence of and easy exploitation of vulnerabilities in software or
1278   hardware. Mitigation of these vulnerabilities may be possible but could prove challenging
1279   due to required coordination with customers, who may be difficult to contact and motivate.
1280   Manufacturers can minimize the impact of support ending for their IoT products by
1281   engaging with customers while also ensuring the final updates maximize on-going
1282   securability of the IoT product. For example, if remote IoT product components (e.g., a
1283   backend) are to be removed when support ends, some or all of the product cybersecurity
1284   capabilities delivered by the backend can be migrated to other IoT product components.

1285   5. **As the IoT product approaches the end of its useful life (i.e., end-of-life), how can the**
1286   **product remain securable?** For some IoT products (e.g., large equipment like vehicles and
1287   appliances), their useful life may far surpass that of the digital technologies the product
1288   uses (i.e., the product may have an extended legacy period). Legacy considerations
1289   highlighted in the previous question related to end-of-support are amplified in this
1290   extended legacy situation, so there may be justification to minimize, or remove entirely,
1291   networking capabilities that provide the IoT product broader internet access.

1292   6. **When an IoT product is no longer securable, how can it be securely decommissioned and**
1293   **disposed of?** Even when used as legacy products, all IoT products will eventually no longer
1294   be useful. This may be because the use case for the product no longer exists or because the
1295   product has failed components that keep it from fulfilling its operational functions. Thus, all
1296   products will eventually need to be fully decommissioned and disposed of in a manner that
1297   preserves the cybersecurity of the product's customers and users. Disposal considerations
1298   are key here since customers will seek to remove or replace these products, which may
1299   have cybersecurity implications. For example, how can data be protected from
1300   unauthorized access after the disposed IoT product leaves the customer's control and
1301   possession.

1302   Agility and adaptability are important to post-market cybersecurity since threats and risks can
1303   change over time due to new vulnerabilities, mitigations, and use cases for IoT products. As in
1304   the pre-market phase, manufacturers and other supporting entities will need to utilize both
1305   technical and non-technical means to ensure on-going securability of IoT products through the
1306   post-market phase.

1307   **4.2. Activity 7: Define Approaches for Communicating to Customers**

1308   For most IoT products and post-market cybersecurity support plans, communication with
1309   customers and other entities within the IoT product's ecosystem is foundational. Clearly
1310   communicating cybersecurity information may necessitate different communication
1311   approaches for different kinds of customers based on their expectations and resources.
1312   Manufacturers can answer questions like the following to help define communication
1313   approaches:

1314   1. **What is the purpose of the communication?** Communicating cybersecurity information
1315   places demands on both the manufacturer and customer. The manufacturer must prepare
1316   and effectively deliver the message while customers must expend time and effort to
1317   understand and decide how to use the information. As such, cybersecurity communications
1318   should be focused on key disclosures or calls for action to customers.

1319   2. **What terminology will the customer understand?** A home user will likely have less
1320   technical knowledge than points of contact at a large business (e.g., system administrators).
1321   For example, IT and cybersecurity professionals may already be familiar with conventions
1322   like referring to a vulnerability by its Common Vulnerabilities and Exposures (CVE) number
1323   while home users likely will not.

1324 3. **How much information will the customer need?** Giving some customers too much
1325   information may overwhelm them and make it harder for them to find the information they
1326   need. Not providing enough information is generally undesirable, except for cases where
1327   revealing the information might have broader negative implications—for example,
1328   publishing technical details of a newly discovered vulnerability before an update is available
1329   to correct the vulnerability.

1330 4. **How/where will the information be provided?** Information can be provided in one or more
1331   logical and/or physical locations. Examples include user manuals, terms of service and other
1332   product documentation, websites, emails, and the IoT product components themselves
1333   (e.g., mobile apps). Customers will benefit more when they can readily locate information
1334   whenever needed.

1335 5. **How can the integrity of the information be verified?** For some methods of providing
1336   information, such as emails, customers may want a way to determine if the information is
1337   legitimate (e.g., not a social engineering attempt).

1338 6. **Will customers need to communicate with the manufacturer?** For example, customers
1339   may seek out updates or other data needed for maintaining their products, including
1340   servicing the IoT device. Customers may also discover vulnerabilities or other issues that
1341   they want to report. The functionality, usability, and efficacy of the communication
1342   channels from customer to manufacturer should be tested by the manufacturer to ensure
1343   customers and others (e.g., security researchers) can make use of the channels.

1344 **4.3. Activity 8: Decide What to Communicate to Customers and How to Communicate It**

1345 There are many potential considerations for what information a manufacturer communicates
1346 to customers for a particular IoT product and how that information will be communicated. The
1347 rest of this section contains examples of topics that manufacturers might want to include in
1348 their communications and, for some examples, thoughts on how that information might be
1349 communicated.

1350 **4.3.1. Cybersecurity Risk-Related Assumptions**

1351 To understand how their risks might differ from the manufacturer's expectations, some
1352 customers may benefit by knowing the cybersecurity-related assumptions the manufacturer
1353 made when designing and developing the product, such as the following:

1354 1. **Who were the expected customers?** Some IoT products are created with a specific sector
1355   or customer type in mind, which could impact not only which product cybersecurity
1356   capabilities are implemented, but also how those capabilities function.

1357 2. **How was the product intended to be used?** Some IoT products have specific intended
1358   purposes when deployed, which can help scope the cybersecurity customers may expect
1359   from the product. Additionally, some IoT products are expected to be used in particular
1360   systems, possibly creating cybersecurity dependencies that customers need to know about

1361   (e.g., a device requires a monitoring system to be able to connect to it for cybersecurity
1362   purposes).

1363   3. **What types of environments would the product be used in?** Customers may need to know,
1364   for example, if an IoT product may not be securable in a public location or without the use
1365   of another device or specific application that provides some or all product cybersecurity
1366   capabilities on behalf of the IoT product. Network bandwidth and latency, as well as other
1367   environmental factors, may also impact which capabilities to incorporate and how to
1368   implement them.

1369   4. **How would responsibilities be shared among the manufacturer, the customer, and others**
1370   **within the IoT product's ecosystem?** Some customers may benefit from knowing if
1371   implementation of product cybersecurity capabilities and related tasks (e.g., software
1372   updates, product configuration, data protection and destruction, and product management)
1373   are the responsibility of one party or multiple parties.

4.3.2. Support and Lifespan Expectations

1375   Communicating product support and lifespan expectations helps customers plan their
1376   cybersecurity risk mitigations throughout the product's support lifecycle, which may be shorter
1377   than how long the customer wants to use the product. To determine what information to
1378   communicate to customers, manufacturers can answer questions like the following:

1379   1. **How long is support for the product intended to be provided?** Telling customers how long
1380   updates and technical support will be available may help them plan to securely use and
1381   maintain products for an appropriate amount of time.

1382   2. **When is it intended for product end-of-life to occur? What will be the process for end-of-**
1383   **life?** Customers may want to retire a product, or at least change how the product is used,
1384   when the manufacturer considers the product and its device component at end-of-life.
1385   These customers may benefit from advance notice (e.g., six months) leading up to that end-
1386   of-life so that they can plan for the event. In some cases, other entities may be the primary
1387   recipient of end-of-life notification. For example, a registry or consortium of registries could
1388   be established to track when products are designated as "end-of-life" by their
1389   manufacturers or such a designation is driven by events (e.g., manufacturer goes out of
1390   business and ceases to exist). Such registries could be the entity informed by manufactures
1391   of when their IoT product is no longer supported, and customers can look to the registries
1392   when researching or maintaining products.

1393   3. **What functionality, if any, will the product have after support ends and at end-of-life?**
1394   Customers may want to know if they will be able to continue use of a product at its end-of-
1395   life, even if cloud-based services or other functions are no longer available. (i.e., will a
1396   freezer continue to function as a freezer even if automatic inventorying applications are not
1397   available)

1398   4. **How can customers report suspected problems with cybersecurity implications, such as**
1399   **software vulnerabilities, to the manufacturer? Will reports be accepted after support**

1400 **ends? Will reports be accepted after end-of-life? Will any action be taken with these**
1401 **reports (e.g., posting to a website) after support ends?** Examples of reporting methods
1402 include phone numbers, email addresses, and web forms.

1403 5. **How can customers maintain securability even after official support for the product has**
1404 **ended (e.g., when a manufacturer or third-party organization with a cybersecurity role**
1405 **shuts down entirely or ends support of the product)? Will essential files or data be made**
1406 **available in a public forum to allow others, even the customers themselves, to continue to**
1407 **support the IoT product?** For example, a manufacturer going out of business may make the
1408 code base of their product available in an open-source repository to allow continued
1409 development and support from the community.

1410 ### 4.3.3. Product Composition and Capabilities

1411 Communicating information about the product's software, hardware, services, functions, and
1412 data types helps customers better understand and manage cybersecurity for their products,
1413 particularly if the customer is expected to play a substantial role in managing cybersecurity. To
1414 determine what information is important to communicate to customers, manufacturers can
1415 answer questions like the following:

1416 1. **What information do customers need on general cybersecurity-related aspects of the**
1417 **product, including installation, configuration (e.g., hardening guide), usage, management,**
1418 **maintenance, and disposal?** Examples include how the product can securely join a system
1419 or network, which configuration options may impact cybersecurity and how they may
1420 impact it, and what ways of using the product are known to be insecure.

1421 2. **What is the potential effect on the product if the cybersecurity configuration is made**
1422 **more restrictive than the default?** Some products may lose some functionality as their
1423 cybersecurity configurations are made more stringent.

1424 3. **What inventory-related information do customers need related to the product's internal**
1425 **software, such as versions, patch status, and known vulnerabilities?** Do customers need to
1426 be able to access the current inventory on demand? Some customers may want to be aware
1427 of known vulnerabilities so they can address them, while other customers may want to
1428 know current software patch status.

1429 4. **What information do customers need about the sources of the product's software,**
1430 **hardware, and services?** Examples of sources include the developer of the product's
1431 software, the manufacturer of the device's processor, and the provider of a cloud-based
1432 service used by the product. Techniques such as a software bill of materials (SBOM) and
1433 hardware bill of materials (HBOM) can be considered as a way to communicate this and
1434 similar information to customers consistently and effectively.

1435 5. **What information do customers need on the product's operational characteristics so they**
1436 **can adequately secure the product?** How should this information be made available? Some
1437 customers may be best served by placing the information on a website, while others may
1438 make best use of the information through a standardized machine-to-machine protocol. In

1439   some cases, such as for device intent signaling, this information or links to it might be best
1440   provided through the product itself.

1441   6. **What functions can the product perform?** This includes not only product cybersecurity
1442   capabilities, but also any other functions that may have cybersecurity implications—for
1443   example, transmitting data to a remote system, or using a microphone and camera to
1444   capture audio and video.

1445   7. **What data types can the product collect?** What are the identities of all parties (including
1446   the manufacturer) that can access that data? Some customers may need to know if location
1447   information or voice commands collected by the product may be stored in a cloud and
1448   accessed for other purposes, possibly by other parties (e.g., for aggregation or analytics).

1449   8. **What are the identities of all entities (including the manufacturer) who have access to or
1450   any degree of control over the product?** For example, a third party providing technical
1451   support on behalf of the manufacturer might be able to remotely update the product's
1452   software and configuration.

1453   4.3.4. Software Updates

1454   Manufacturers communicating information about software updates helps customers plan their
1455   cybersecurity risk mitigations and maintain the cybersecurity of their products, particularly in
1456   response to emerging threats. Updating the software on the IoT device component of the
1457   product can require customer action or be more specialized than that for other product
1458   components. To determine what update information is important to communicate to
1459   customers, manufacturers can answer questions like the following:

1460   1. **Will updates be made available? If so, when will they be released?** Knowing if updates will
1461   be provided on a set schedule or sporadically will help customers plan for applying them.

1462   2. **Under what circumstances will updates be issued?** Examples include controlling the
1463   execution of faulty software and correcting a previously unknown vulnerability in a standard
1464   protocol.

1465   3. **How will updates be made available or delivered? Will there be notifications when
1466   updates are available or applied?** Customers can better plan for applying updates if they
1467   know they must be downloaded through a specific portal and applied to the device.
1468   Customers may also benefit from being notified that an update has to be or has been
1469   applied, even in cases where the delivery and application of the software update is
1470   automatic, over-the-air, and requires no action from the customer or users.

1471   4. **Which entity (e.g., customer, manufacturer, maintainer) is responsible for performing
1472   updates? Or can the customer designate which entity will be responsible (e.g.,
1473   automatically applied by the manufacturer)? Do responsibilities vary for different IoT
1474   product components?** Some customers may benefit from knowing that certain IoT device
1475   updates will be available from a third party and that other updates will be provided by the
1476   manufacturer. Some customers may likewise benefit from being made aware of their roles,
1477   responsibilities, and options regarding updates. This will likely vary for different IoT product

1478   components. For example, IoT devices may be managed by customers in many cases, but
1479   most backends will not.

1480   5. **How can customers verify and authenticate updates? Can verification and authentication**
1481   **of updates be achieved automatically by the IoT product?** Examples are cryptographic hash
1482   comparison, code signature validation, and reliance on manufacturer-provided software
1483   that automatically performs update verification and authentication.

1484   6. **What information should be communicated with each individual update?** Examples
1485   include the reason for the update (e.g., corrections to errors, altered or new capabilities)
1486   and any effect installing the update could have on a customer's existing configuration
1487   settings.

1488   ### 4.3.5. Product Retirement Options

1489 Customers are more effectively able to plan when manufacturers communicate information
1490 about product retirement options (e.g., the ability to "decommission" the product). To
1491 determine what information about product retirement options is important to communicate to
1492 customers, manufacturers can answer questions like the following:

1493   1. **Will customers want to transfer ownership of their IoT products to another party? If so,**
1494   **what do customers need to do so their user and configuration data on the IoT product are**
1495   **not accessible by the party who assumes ownership?** For example, a customer may want
1496   to sell a facility that contains smart building automation devices and would want a way to
1497   ensure all data has been removed from the devices before the buyer gains access to them.

1498   2. **Will customers want to render their devices inoperable? If** so, how can customers do that?
1499   Some IoT devices can be rendered inoperable through logical means (e.g., as executed
1500   through a mobile app), while others use physical means (e.g., a button on the device).

1501   ### 4.3.6. Technical and Non-Technical Cybersecurity Capabilities

1502 Communicating information about the product's cybersecurity capabilities, the non-technical
1503 means provided by the manufacturer or other entities, and the non-technical means customers
1504 may need to perform themselves, helps customers better understand how to manage risk for
1505 the product. To determine what information about product cybersecurity capabilities is
1506 important to communicate to customers, manufacturers can answer questions like the
1507 following:

1508   1. **Which product cybersecurity capabilities can be provided:**

1509   a. **by the device itself (device cybersecurity capabilities)?** Examples include encryption
1510   used by the device for data protection, the presence of a physical identifier on the
1511   device, and authentication and authorization mechanisms the device uses to limit
1512   access to its network interfaces.

1513   b. **by other local product components?** Some technical means may be delivered or
1514   supported by an IoT hub or mobile app that is part of the IoT product.

1515   c. **by a manufacturer service, system or other remote product components?** An example
1516   would be technical means provided by an internet server or cloud-hosted service.

1517 2. **Which non-technical means can be provided by the manufacturer or other organizations**
1518   **and services acting on behalf of the manufacturer?** Examples include many of the concepts
1519   discussed throughout this section, such as lifespan expectation, software update plans, and
1520   retirement options. In addition to those discussed in this section, there may also be other
1521   non-technical means (e.g., how a flaw or vulnerability may be reported) customers would
1522   benefit from knowing about and understanding.

1523 3. **Which technical or non-technical means should the customer provide themselves or**
1524   **consider providing themselves?** Examples would be using network-based security controls
1525   (e.g., a firewall) to prevent direct access to local IoT product components from the internet
1526   and performing audits of the implementation and settings to ensure compliance
1527   requirements are met.

1528 4. **How is each of the technical and non-technical means expected to affect cybersecurity**
1529   **risks?** For example, proper implementation of data protection may help mitigate
1530   confidentiality risks, but may also reduce availability (e.g., if data cannot be decrypted or is
1531   decrypted slowly).

1532   **5. Conclusion**

1533   This publication discusses nine cybersecurity-related activities for IoT product manufacturers
1534   and gives examples of questions manufacturers can answer for each activity. Manufacturers
1535   who choose to perform one or more of these foundational cybersecurity activities should
1536   determine the applicability of the example questions and identify any other questions that may
1537   help to understand customers' cybersecurity needs and goals, including the product
1538   cybersecurity capabilities their customers expect. The questions highlighted for each activity
1539   are meant as a starting point and do not entirely define each activity. Also, the process
1540   described in this publication is not meant to imply that the role of manufacturers is limited to
1541   providing capabilities that require action by customers, but rather should drive manufacturers
1542   to better understand their customers' needs and goals in the context of the IoT product, which
1543   may require automated capabilities, and/or additional supporting non-technical actions. For
1544   some customers and use cases, where it is possible and appropriate, limited customer
1545   responsibility for cybersecurity may lead to better cybersecurity outcomes for the ecosystems
1546   than if the burden was left fully on customers.

References

[1]   Executive Order no. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, DCPD-201700327, May 11, 2017. https://www.govinfo.gov/app/details/DCPD-201700327

[2]   Executive Order no. 14028, *Improving the Nation's Cybersecurity*, 86 FR 26633, May 12, 2021. https://www.govinfo.gov/app/details/FR-2021-05-17/2021-10460

[3]   Internet of Things Advisory Board (2024) Internet of Things (IoT) Advisory Board (IoTAB) Report. (National Institute of Standards and Technology, Gaithersburg, MD). https://www.nist.gov/system/files/documents/2024/10/21/The%20IoT%20of%20Things%20Oct%202024%20508%20FINAL_1.pdf

[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 Revision 2. https://doi.org/10.6028/NIST.SP.800-37r2

[5]   Joint Task Force (2020) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Revision 5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[6]   Simmon, E (2020) Internet of Things (IoT) Component Capability Model for Research Testbed. (National Institute of Standards and Technology, Gaithersburg, MD), NIST IR 8316. https://doi.org/10.6028/NIST.IR.8316

[7]   Voas JM (2016) Networks of 'Things'. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-183. https://doi.org/10.6028/NIST.SP.800-183

[8]   National Institute of Standards and Technology (2024) Framework for Improving Critical Infrastructure Cybersecurity, Version 2.0. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.29

[9]   Boeckl K, Fagan M, Fisher W, Lefkovitz N, Megas K, Nadeau E, Piccarreta B, Gabel O'Rourke D, Scarfone K (2019) Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8228. https://doi.org/10.6028/NIST.IR.8228

[10]   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

[11]   Fagan M, Megas KN, Marron J, Brady KG, Cuthill B, Herold R (2021) IoT Non-Technical Supporting Capability Core Baseline. (National Institute of Standards and Technology) NIST Internal Report (IR) 8259B. https://doi.org/10.6028/NIST.IR.8259B

[12]   Stouffer K, Pillitteri V, Lightman S, 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

1587 [13] Cyber-Physical Systems Public Working Group (2017) Framework for Cyber-Physical
1588   Systems: Volume 1, Overview, Version 1.0. (National Institute of Standards and
1589   Technology, Gaithersburg, MD), NIST Special Publication (SP) 1500-201.
1590   https://doi.org/10.6028/NIST.SP.1500-201

1591 [14] Merriam-Webster (2017) Webster's Third New International Dictionary Unabridged.
1592   (Merriam-Webster, Springfield, MA).

1593 [15] Dodson D, Souppaya M, Scarfone K (2019) Mitigating the Risk of Software Vulnerabilities
1594   by Adopting a Secure Software Development Framework (SSDF). (National Institute of
1595   Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper.
1596   https://csrc.nist.gov/publications/detail/white-paper/2020/04/23/mitigating-risk-of-
1597   software-vulnerabilities-with-ssdf/final

1598 [16] Boyens JM, Smith AM, Bartol N, Winkler K, Holbrook A, Fallon M (2022) Cybersecurity
1599   Supply Chain Risk Management Practices for Systems and Organizations. (National Institute
1600   of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-
1601   161r1-upd1, Includes updates as of November 01, 2024.
1602   https://doi.org/10.6028/NIST.SP.800-161r1-upd1

1603 [17] Fagan M, Megas KN, Marron J, Brady KG, Jr., Herold R, Lemire D, Hoehn, B (2021). IoT
1604   Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device
1605   Cybersecurity Requirements. (National Institute of Standards and Technology,
1606   Gaithersburg, MD), NIST Special Publication (SP) 800-213.
1607   https://doi.org/10.6028/NIST.SP.800-213

1608 [18] Fagan M, Megas KN, Marron J, Brady KG, Jr., Herold R, Lemire D, Hoehn, B (2021). IoT
1609   Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity
1610   Requirement Catalog. (National Institute of Standards and Technology, Gaithersburg, MD),
1611   NIST Special Publication (SP) 800-213A. https://doi.org/10.6028/NIST.SP.800-213A

1612 [19] IEC 81001-5-1:2021, Health software and health IT systems safety, effectiveness and
1613   security – Part 5-1: Security — Activities in the product life cycle.
1614   https://www.iso.org/standard/76097.html

1615 [20] ANSI/ISA-62443-4-1-2018, Security for Industrial Automation and Control Systems – Part 4-
1616   1: Secure Product Development Lifecycle Requirements.
1617   https://www.isa.org/products/ansi-isa-62443-4-1-2018-security-for-industrial-au

1618 [21] Fagan M, Megas KN, Watrobski P, Marron J, Cuthill B (2022) Profile of the IoT Core Baseline
1619   for Consumer IoT Products. (National Institute of Standards and Technology, Gaithersburg,
1620   MD), NIST IR 8425. https://doi.org/10.6028/NIST.IR.8425

1621 [22] National Institute of Standards and Technology (2023) Artificial Intelligence Risk
1622   Management Framework, Version 1.0. (National Institute of Standards and Technology,
1623   Gaithersburg, MD), NIST Trustworthy and Responsible AI (AI) NIST AI 100-1
1624   https://doi.org/10.6028/NIST.AI.100-1

1625 [23] National Institute of Standards and Technology (2020) NIST Privacy Framework: A Tool for
1626   Improving Privacy Through Enterprise Risk Management, Version 1.0. (National Institute of
1627   Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP)
1628   NIST CSWP 10. https://doi.org/10.6028/NIST.CSWP.10

1629 [24] Temoshok D, Proud-Madruga D, Choong Y-Y, Galluzzo R, Gupta S, LaSalle C, Lefkovitz NB,
1630   Regenscheid AR (2025) Digital Identity Guidelines. (National Institute of Standards and

1631   Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63-4.
1632   https://doi.org/10.6028/NIST.SP.800-63-4

Appendix A. List of Abbreviations and Acronyms

API
Application Programming Interface

CVE
Common Vulnerabilities and Exposures

FISMA
Federal Information Security Modernization Act

FOIA
Freedom of Information Act

HBOM
Hardware Bill of Materials

ICS
Industrial Control System

IoT
Internet of Things

IP
Internet Protocol

IR
Internal Report

IT
Information Technology

ITL
Information Technology Laboratory

LTE
Long-Term Evolution

MAC
Media Access Control

NIST
National Institute of Standards and Technology

SBOM
Software Bill of Materials

SDK
Software Development Kit

SP
Special Publication

SSDF
Secure Software Development Framework

September 2025

Foundational Cybersecurity Activities
for IoT Product Manufacturers

1670 **USB**
1671 Universal Serial Bus

1672 **UWB**
1673 Ultra-Wideband

1674 **Wi-Fi**
1675 Wireless Fidelity

1676   **Appendix B. Glossary**

1677   **Actuator**
1678   A portion of an IoT device capable of changing something in the physical world. [6]

1679   **Device Cybersecurity Capability Core Baseline**
1680   A set of technical device capabilities needed to support common cybersecurity controls that protect the
1681   customer's devices and device data, systems, and ecosystems. [10]

1682   **Device Cybersecurity Capability**
1683   A cybersecurity feature or function provided by an IoT device through its own technical means (i.e., device
1684   hardware and software).

1685   **IoT Device**
1686   Devices that have at least one transducer (sensor or actuator) for interacting directly with the physical world and
1687   at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth) for interfacing with the digital world.

1688   **IoT Non-Technical Supporting Capability Core Baseline**
1689   A set of non-technical supporting capabilities generally needed from manufacturers or other third parties to
1690   support common cybersecurity controls that protect an organization's devices as well as device data, systems, and
1691   ecosystems. [11]

1692   **IoT Platform**
1693   A piece of IoT device hardware with supporting software already installed and configured for a manufacturer's use
1694   as the basis of a new IoT device. An IoT platform might also offer third-party services or applications, or a software
1695   development kit to help expedite IoT application development.

1696   **IoT Product**
1697   An IoT device or IoT devices and any additional product components (e.g., backend, mobile app) that are necessary
1698   to use the IoT device beyond basic operational features.

1699   **IoT Product Component**
1700   An IoT device or other digital equipment or service (e.g., backend, mobile app) used to create IoT products.

1701   **IoT System**
1702   Networked computing resources combined with sensors and actuators. [6]

1703   **Means**
1704   An agent, tool, device, measure, plan, or policy for accomplishing or furthering a purpose. [14] In the context of
1705   this publication, we discuss technical means, which come from hardware and software, as well as non-technical
1706   means, which come from actions and procedures.

1707   **Securable IoT Product**
1708   An IoT product that has product cybersecurity capabilities (i.e., hardware and software) and other support
1709   provided by the manufacturer or other supporting entity that customers may need to mitigate common and
1710   expected cybersecurity risks related to the use of the IoT product and its connection to customers' systems.

1711   **Network Interface**
1712   An interface that connects an IoT device to a network (e.g., Ethernet, Wi-Fi, Bluetooth, Long-Term Evolution [LTE],
1713   Zigbee, Ultra-Wideband [UWB]).

1714   **Product Cybersecurity Capability**
1715   A cybersecurity feature or function provided by an IoT product through its own technical means via one or more
1716   components (i.e., IoT platform, cloud backend, device hardware and software).

1717   **Sensor**

1718   A portion of an IoT device capable of providing an observation of an aspect of the physical world in the form of
1719   measurement data. [6]

1720   **Transducer**
1721   A portion of an IoT device capable of interacting directly with a physical entity of interest. The two types of
1722   transducers are sensors and actuators. [9]

Appendix C. Change Log

NIST IR 8259 was originally published as final in May 2020. To ensure the guidelines are timely, useful, and effective, NIST has spent the time from December 2024 until May 2025 to revisit NIST IR 8259, determine potential areas of revision, engage with the IoT cybersecurity community. The Initial Public Draft for NIST IR 8259 Rev. 1 published on May 13, 2025, with comments closing on July 14, 2025. From the written comments and comments at a June 19, 2025 discussion forum on the draft, NIST has chosen to issue a second public draft. The following areas have been revised from Initial Public Draft NIST IR 8259 Revision 1:

- Within the executive summary, clarification that while the activities in the publication are intended to be performed sequentially but some may also be performed in parallel and that the activities are not mapped to an organizational structure to allow the flexibility of the manufacturer organization to align across multiple individuals and departments with roles and responsibilities in adopting the activities.

- Clarifications in Section 2 of the following:

    o Within Section 2.2 **Composition of IoT Products**

        – Ending paragraphs and large callout box on IoT products' technical means discussion was removed.

    o Within Section 2.3 **Entities in an IoT Product Ecosystem**

        – Paragraph on IoT product ecosystems was added with examples.

        – Paragraph added to indicate that not all entities that interact with IoT products have the same impact on and relationship with cybersecurity related to the IoT product.

    o Within Section 2.4 **The Role of the Manufacturer in Cybersecurity**

        – The addition of a table with the Activities and Example Outputs was added for clarity

        – Within Access Management – Clarification on limits on access privileges and following the principle of least privilege.

        – The removal of a paragraph on cybersecurity needs and goals incorporating product cybersecurity capabilities and risk mitigation context. (further clarified below)

    o Within Section 2.6 **Relationships between Needs and Goals, Capabilities, and Means**

        – New section pulling the removal of the content from 2.4 down and expanding. Clarification added on customers using means to achieve their needs and goals leading into the Figure 4 (that already existed but was moved up from Activity 4) on how various means are implemented by different IoT components and ecosystem entities.

- 1760   – Following the diagram, more clarification on technical means, how NIST
- 1761   defines a capability and product cybersecurity capabilities. Paragraph on IoT
- 1762   product components having different resources and capabilities with
- 1763   examples. Paragraph supporting what product non-technical supporting
- 1764   capabilities are and examples. Includes a new table 2 – Examples
- 1765   demonstrating relationship among customer needs and goals, product
- 1766   cybersecurity capabilities, and means. Indicates that throughout the rest for
- 1767   the publication the activities which include technical means and non-means
- 1768   are expressed through product cybersecurity capabilities and device
- 1769   cybersecurity capabilities.

- 1770 • Within Section 3, changed the following:

- 1771   o Added "Activity 0: Prioritize Cybersecurity and Maintain Cybersecurity Posture" to
- 1772   clarify that manufacturing organizations need cybersecurity to be a focus of the
- 1773   product development process. This activity is added because it's been assumed
- 1774   implicitly this activity 0 has been taken by manufacturers to prioritize and maintain
- 1775   their organizational cybersecurity posture. And some organizations may have limited
- 1776   cybersecurity experience for a variety of reasons.

- 1777   o **Updates to** questions beginning that cybersecurity risk discussion (1-5 sourced from
- 1778   CSF):

- 1779   – Highlighting manufacturers can utilize tools such as the MITRE ATT&CK or
- 1780   EMB3D Frameworks to identify applicable threats.

- 1781   – Focusing on how the organization assess and mitigate cybersecurity risks by
- 1782   adding Added context that it's critical that IoT product manufactures aim for
- 1783   a strong cybersecurity posture with an indication that standards and tools
- 1784   exist to aid and references CSF, RMF and ISA/IEC 62443.

- 1785   o Added considerations for developers and manufacturers and references for Secure
- 1786   Software Development Framework and NIST SP 800-161 rev 1 on supply chain risk
- 1787   management.

- 1788   o Closing paragraph indicating the rest of the activities concern the cybersecurity of
- 1789   IoT products rather than the cybersecurity posture of IoT manufacturers. This allows
- 1790   focus on the cybersecurity of their customers.

- 1791   o Within Section 3.2 **Activity 1: Identify Expected Customers and Define Expected**
- 1792   **Use Cases**, the following were updated:

- 1793   – First sentence added to clarify that Manufacturers should look to many
- 1794   sources for determining their IoT product requirements but one key source is
- 1795   the customer's needs and goals.

- 1796   – Defining requirements was removed.

- 1797   o Within Section 3.3**. Activity 2: Research Customer Cybersecurity Needs and Goals**

- 1798   – The callout box referencing Fig 4 was removed.

1799
1800

– The figure 4 title was updated – Cybersecurity Connections between IoT
product manufacturers and customers.

1801

– Paragraph was added in the to clarify the purpose of the questions.

1802
1803

– Following the paragraph on FDA/HIPAA – example voluntary consensus
standards and international schemes were added including:

1804
1805

- Healthcare: Part 5-1: Security — Activities in the product life cycle, IEC
810015-1.

1806
1807

- Industrial: Part 4-1: Secure product development lifecycle
requirements, ISA/IEC 62443-4-1

1808
1809

- Cyber Security Agency of Singapore's Cybersecurity Labelling Scheme
or the European Union's Cyber Resilience Act.

1810

- Fig 5. Text updated.

1811
1812
1813

o Split "Activity 3" in the initial public draft into two activities ("Activity 3" and
"Activity 4") and renumbered other activities and related subsections accordingly.
This was to focus greater attention on establishing cybersecurity requirements.

1814
1815
1816

o Within Section 3.4 Activity 3 title updated to **Activity 3: Determine Appropriate
Means Support Customer Needs and Goals in the Context of the IoT Product,** the
following were updated:

1817
1818
1819
1820
1821
1822

– Description updated to consider other factors in addition to customer
cybersecurity needs and goals with inclusion of diagram on Maintenance
Needs and Expectations, Product Functions and Features inclusive of Product
Cybersecurity Capabilities (technical means device, technical means product
components, non-technical means from supporting entities) and Product
Operational Capabilities. Also, Physical Attributes and Human Factors.

1823
1824
1825
1826

– Three paragraphs added to explain how factors related to IoT products stack,
that factors need to be aligned with and support customer needs and goals,
and this understanding gained can help determine how to support
cybersecurity.

1827
1828
1829
1830
1831

– Added a new paragraph at the end: Not all means will be applicable for the
IoT product. Customers may have needs and goals that cannot be supported
due to limitations. Contractual, regulatory, or legal obligations may also limit
means. Manufacturers should consider all sources for limitations on means
for their customer's needs and goals.

1832
1833
1834
1835
1836
1837

– Several examples were added following the last paragraph preceding a new
Fig 7 on how manufacturers should consider sources and limitations on
means when determining what the customer will need and expect to support
customer needs and goals (supply chains, ecosystem obligations, physical
product considerations, and IoT product lifecycle and maintenance
expectations).

1838   – Added description to Fig 7 'Various factors combine to influence appropriate
1839   and applicable means for cybersecurity' which illustrates how factors collide
1840   to shape an IoT product's technical and non-technical means for
1841   cybersecurity.

1842   – Added a paragraph following Fig 7 on: Manufacturers could use an
1843   understanding of means to document and express cybersecurity support aim
1844   to provide for the product. This can enable a broader view of cybersecurity
1845   through the product's lifecycle and better communication about
1846   cybersecurity features with ecosystem entities.

1847   o Within Section 3.5 **Activity 4 - Define IoT Product Cybersecurity Capabilities Based**
1848   **on Appropriate Means,** figure was removed and moved to Section 2.

1849   o Within 3.6 Activity 5: Plan for Adequate Support of Customer Needs and Goals, the
1850   following were updated:

1851   – Greater discussion of how IoT product manufacturers should consider that
1852   their decisions can have impacts on secureability and that they should make
1853   decisions to support all stags of IoT product's lifecycle

1854   – An example on post-quantum cryptography was added to question 3.

1855   – A new question and context were added to address new areas and risk
1856   considerations such as the inclusion of AI.

1857 • Within Section 4, there were the following updates:

1858   o Within Section 4.1 **Activity 6: On-Going Support of Product Cybersecurity through-**
1859   **out the Lifecycle and through End-of-Life**, the following were updated:

1860   – The activity title was updated.

1861   – Question 5 was clarified by removing the final portion and creating a new
1862   question 6.

1863   – Additional context was added to question 6, to further expand on
1864   decommissioning and disposal.

1865   o Within Section 4.3.2 **Support and Lifespan Expectations**, the following were
1866   updated:

1867   – Question 2 was updated with a new discussion around different options at
1868   "end of life" of the product. The new paragraph discusses notifications,
1869   registries and related information.

1870

1871 Beyond these technical revisions, edits have been made throughout the document to clarify
1872 language and concepts, including additional figures, removing or revising confusing phrasing,
1873 and updating some examples given to demonstrate concepts. References were also updated to
1874 reflect current versions of documents and new related documents published since May 2020.