NIST Internal Report
NIST IR 8259r1

Foundational Cybersecurity Activities for IoT Product Manufacturers

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

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8259r1

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

NIST Internal Report
NIST IR 8259r1

Foundational Cybersecurity Activities for IoT Product Manufacturers

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

Brad Hoehn
Electrosoft

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8259r1

April 2026

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

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

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

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

Publication History
Approved by the NIST Editorial Review Board on 2026-04-09
Supersedes NIST IR 8259 (May 2020) https://doi.org/10.6028/NIST.IR.8259

How to Cite this NIST Technical Series Publication
Fagan M, Megas K, Cuthill B, Marron J, Hoehn B (2026) Foundational Cybersecurity Activities for IoT Product Manufacturers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8259r1. https://doi.org/10.6028/NIST.IR.8259r1

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

Contact Information
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/final, including related content, potential updates, and document history.

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

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.

Keywords

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

Reports on Computer Systems Technology

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

Table of Contents

List of Figures

Acknowledgments

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

Executive Summary

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

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

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

1. Introduction

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

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

1.1. Purpose and Scope

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

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

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

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

1. When considering that IoT products will be attached to networks and primarily managed by customers when deployed, IoT product manufacturers cannot create something that is secure in an absolute sense, but rather securable by customers in deployment.
2. Secure operation of IoT products is only part of the scope of this document, and this document also addresses how IoT products should support the cybersecurity of customers and the systems they attach to.

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

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

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

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

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

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

1.2. Publication Structure

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

- Section 2 provides background information needed to understand the seven recommended pre-market and post-market activities described in Sections 3 and 4.
- Section 3 includes recommended manufacturer activities that primarily impact securability efforts by the manufacturer before sale (i.e., premarket). The Section 3 activities are:
    - Activity 0: Prioritize Cybersecurity and Maintain Cybersecurity Posture.
    - Activity 1: Identify Expected Customers and Define Expected Use Cases.
    - Activity 2: Research Customer Cybersecurity Needs and Goals.
    - Activity 3: Determine Appropriate Means to Support Customer Needs and Goals in the Context of the IoT Product.
    - Activity 4: Define IoT Product Cybersecurity Capabilities Based on Appropriate Means.
    - Activity 5: Plan for Adequate Support of Customer Needs and Goals.
- Section 4 includes recommended manufacturer activities that primarily impact securability efforts by the manufacturer after sale (i.e., post-market). The Section 4 activities are:
    - Activity 6: On-Going Support of Product Cybersecurity through-out the Lifecyle and through End-of-Life.
    - Activity 7: Define Approaches for Communicating to Customers.
    - Activity 8: Decide What to Communicate to Customers and How to Communicate It.
- Section 5 provides a conclusion for the publication.
- The References section lists the references for the publication.
- Appendix A provides a list of acronyms and abbreviations used in the publication.
- Appendix B contains a glossary of selected terms used in the publication.
- Appendix C presents changes that were made to the original NIST IR 8259 report in writing this Initial Public Draft.

2. Background

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

2.1. Product Cybersecurity and System Cybersecurity

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

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

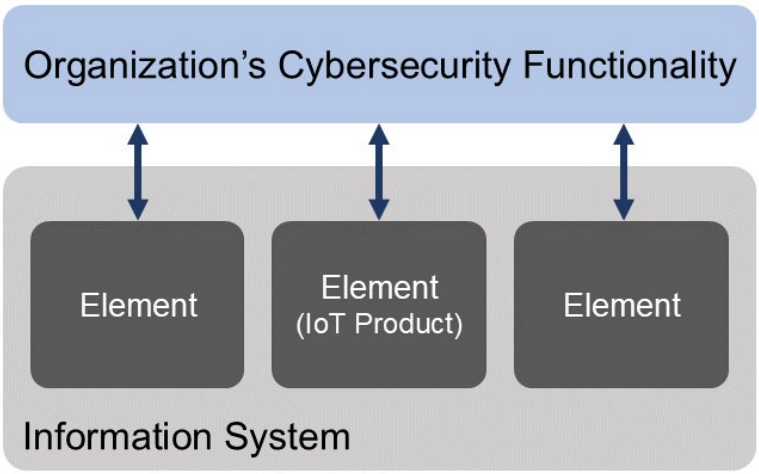

Figure 1. Relationship of organizational information system elements to an organization's cybersecurity.

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

2.2. Composition of IoT Products

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

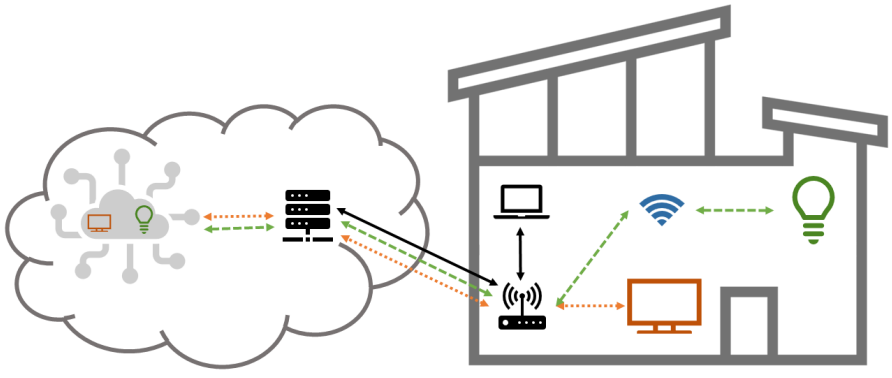

Figure 2. Example of a network showing multiple IoT products based around different IoT devices which are supported by various kinds of IoT product components.

Figure 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 resources 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, and 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

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

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

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

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	Example Output
	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*

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

2.5. IoT Product Customer Cybersecurity Needs and Goals

Improving the securability of an IoT product means helping customers meet their cybersecurity needs and goals. All customers will have cybersecurity needs and goals, but the specific cybersecurity needs and goals for a customer of an IoT product will be dependent on the threats faced by the product and risks potentially associated with the product. The needs and goals will also be framed and informed by the customer's knowledge, expectations, etc. Addressing cybersecurity needs and goals should be risk-based. Even customers without formal risk mitigation goals, such as home consumers, will care about cybersecurity threats and often have informal and indirect cybersecurity goals. At the least, customers will want their IoT products to provide desired functionality as expected (e.g., automatically), which is dependent on addressing threats the product faces that could impact functionality. Thus, customers may expect that adequate cybersecurity measures are available or in place to protect them and the product's desired functionality.

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

- **Asset Management:** Maintain a current, accurate inventory of all IoT products and their relevant characteristics throughout the products' lifecycles[2] in order to use that information for cybersecurity risk management purposes. Being able to distinguish each IoT product deployment from all others is needed for the other common risk mitigation areas, such as vulnerability management, access management, data protection, and incident detection.
- **Vulnerability Management:** Identify and mitigate known vulnerabilities in the software of IoT devices and other IoT product components throughout the IoT products' lifecycles in order to reduce the likelihood and ease of exploitation and compromise. Vulnerabilities can be eliminated by installing updates (e.g., patches) and changing configuration settings. Updates can also correct IoT product operational problems, which can improve availability, reliability, performance, and other aspects of product operation. Customers often want to alter configuration settings for a variety of reasons, including improving or customizing cybersecurity, interoperability, privacy, performance, and usability features. Criticality is important to consider with respect to vulnerabilities since critical vulnerabilities may necessitate a temporary mitigation for customers while an update is developed.
- **Access Management:** Prevent unauthorized and improper physical and logical access to, usage of, and administration of IoT products throughout their lifecycles by people, processes, and other computing devices. This includes limits on access privileges for the manufacturer themselves, as well as other entities who may interact with the IoT product

[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.)

such as bystanders and maintainers. Following the principle of least privilege, all authorized entities should have a clear and distinct purpose for access, and their access should be strictly limited to what is necessary for the purpose. Limiting access to interfaces reduces the attack surface of the product, giving attackers fewer opportunities to compromise it. For the IoT device component of the product, this includes physical interfaces.

- **Data Protection:** Prevent access to and tampering with data at rest or in transit that might expose sensitive information or allow manipulation or disruption of IoT product operations throughout the lifecycle including at disposal.
- **Incident Detection:** Monitor and analyze IoT product activity for signs of incidents involving data security across IoT products' components and throughout the products' lifecycles. These signs can also be useful in investigating compromises and troubleshooting certain operational problems.

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

> For many IoT products, additional types of risks, such as privacy,[3] safety, reliability, or resiliency, need to be managed simultaneously with cybersecurity risks because addressing one type of risk can have impacts on others. A common example is ensuring that when a product fails, it does so in a safe manner. Only cybersecurity risks are discussed in this publication. Readers who are interested in better understanding other types of risks and their relationship to cybersecurity may benefit from reading NIST SP 800-82 Revision 3, *Guide to Operational Technology (OT) Security* [12], NIST SP 1500-201, *Framework for Cyber-Physical Systems: Volume 1, Overview, Version 1.0* from the Cyber-Physical Systems Public Working Group [13], NIST IR 8286 Revision 1, *Integrating Cybersecurity and Enterprise Risk Management (ERM)* [14], NIST SP 800-221 *Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs within an Enterprise Portfolio* [15], and NIST SP 800-221A *Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio* [16].

[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.

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

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

In practice, customers will use means to achieve their needs and goals. Means is defined as "an agent, tool, device, measure, plan, or policy for accomplishing or furthering a purpose." [17] This publication refers to technical or non-technical means for cybersecurity purposes, whether performed by an IoT product itself or from supporting entities. Customers will rely on these means to plan for and maintain the cybersecurity of the product within their systems and environments. Figure 3 depicts how various kinds of means, implemented by different IoT product components and ecosystem entities comprise product cybersecurity capabilities.

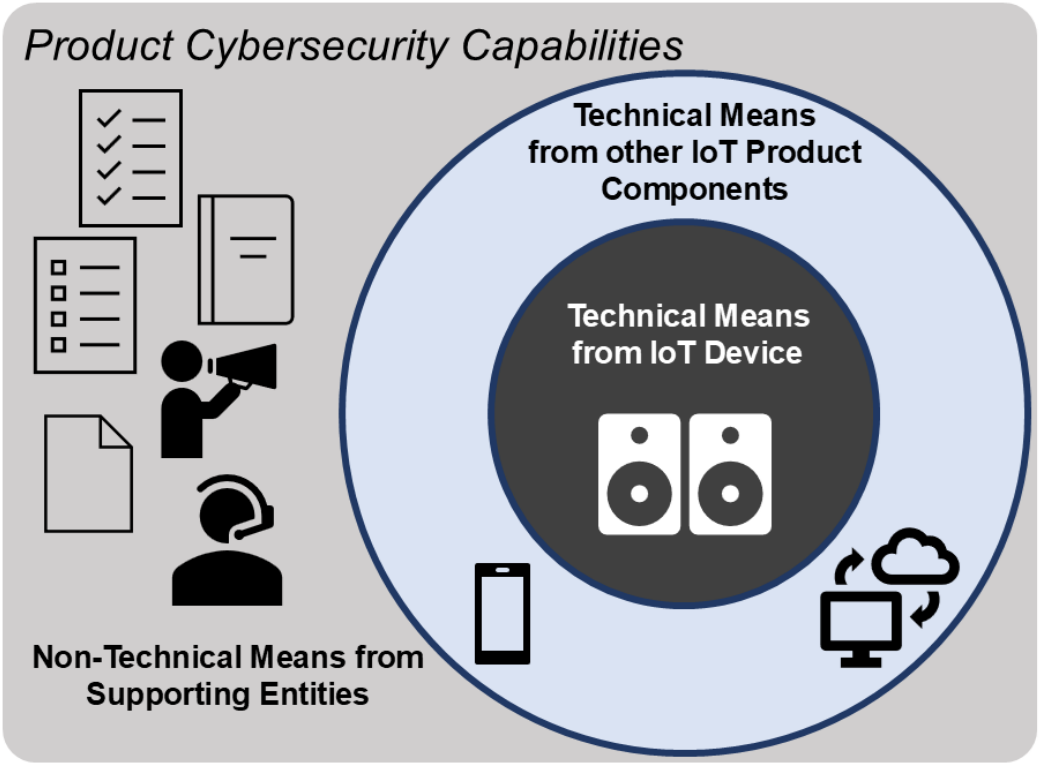

Figure 3. Technical and non-technical means that can support cybersecurity of IoT products provided as product cybersecurity capabilities.

IoT products' technical means (shown within co-centric circles in Fig. 3) will define product cybersecurity capabilities to support the cybersecurity of the networks to which they are eventually attached. In general, NIST has defined a capability as "a combination of mutually

reinforcing controls implemented by technical means, physical means, and procedural means." [4] More specifically, product cybersecurity capabilities are capabilities aligned with this definition but provided by or related to the IoT product. IoT device cybersecurity capabilities are capabilities provided by the IoT device specifically (i.e., cybersecurity features or functions the device provides through its own technical means). Other IoT product components may also contribute to IoT product cybersecurity capabilities through their technical means.

IoT product components will have different resources and capabilities available and, thus, different ways they will contribute to product cybersecurity capabilities. Some product cybersecurity capabilities will be supported similarly by most IoT product components. For example, data protection will use the same or similar means across IoT product components to protect data at rest and in transit. Other product cybersecurity capabilities may be supported differently by various IoT product components. For example, controlling access to interfaces may use similar means (e.g., passwords) for an IoT device and its backend, but the IoT device may have local interfaces whereas the backend may have remotely accessible interfaces. Finally, some product cybersecurity capabilities may be supported entirely differently by different IoT product components. For example, software updates will be managed on the IoT device through potentially automated systems and the customer; however, backend software updates will be managed by the administrator of the backend.

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

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

Table 2. Examples demonstrating relationship among customer needs and goals, product cybersecurity 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.

Rather than discuss technical and non-technical means exclusively, this publication will also refer to product cybersecurity capabilities and device cybersecurity capabilities. In many cases, technical and non-technical means can be easier to identify to satisfy a customer's cybersecurity needs and goals, but product cybersecurity capabilities allow for the IoT product manufacturer to express how the IoT product supports cybersecurity when the specific means may be indeterminate. For example, product cybersecurity capabilities may be more useful than means to describe the cybersecurity features when different means are used for different customers or deployments. For some entities, including many customers, specific means are immaterial to the product cybersecurity capabilities provided. Finally, in discussion of these concepts for the purposes of this publication, where complete and specific details about IoT products are not possible, it is easier to generalize expectations around cybersecurity at the level of product and device cybersecurity capabilities rather than specific technical and non-technical means. Nonetheless, in all cases where any of these terms are used, readers should keep their relationship in mind.

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

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

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

3.1. Activity 0: Prioritize Cybersecurity and Maintain Cybersecurity Posture

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

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

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

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

1. **How does my organization identify cybersecurity threats and risks?** Manufacturers can utilize tools such as the MITRE ATT&CK or EMB3D Frameworks to identify applicable threats to both their operations and systems, as well as to their IoT products in deployment.
2. **How does my organization assess and mitigate cybersecurity risks we face?** It is critical that IoT product manufacturers aim for a strong cybersecurity posture by proactively protecting their operations and systems from cybersecurity attacks. Many standards and other tools exist to aid organizations, including IoT product manufacturers, in the assessment of cybersecurity risk and selection of appropriate mitigations. For example, organizations can look to the Cybersecurity Framework (CSF), Risk Management Framework (RMF), and the ISA/IEC 62443 series, to name a few.
3. **What are effective means that my organization can use to monitor for potential cybersecurity attacks and detect when a cybersecurity attack may be underway?** Risk management is an on-going process, and so manufacturers should implement cybersecurity controls that help them monitor their operations and systems and identify signs of cybersecurity attacks.
4. **When there is a cybersecurity attack, what are my organization's response and recovery plans?** Cybersecurity attacks are not always stopped by existing controls, and so manufacturers should be prepared to respond and recover from their impacts. For example, regularly backing up systems and their data can help an organization respond to a ransomware attack or natural disaster.
5. **What are ways all parts of my organization contribute to our cybersecurity posture?** Cybersecurity should not be siloed to one team or division. Organizations run on digital technologies, and so cybersecurity should be considered across all units. [14] Therefore, cybersecurity activities (e.g., awareness training) should engage the whole organization.
6. **Are there cybersecurity considerations for my organization based on our role as an IoT product developer and manufacturer?** Cybersecurity considerations for developers and manufacturers can be distinct in some ways from cybersecurity considerations for organizations in general. Tools such as the Secure Software Development Framework (SSDF) [18] can help software developers, including IoT product manufacturers. Cybersecurity of the supply-chain for an IoT product, including portions of the development or support of the IoT product by other parties, is also important for IoT product manufacturers to

consider. Manufacturers can refer to *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, SP 800-161 Rev. 1 [19] for additional information about supply-chain risk management.

Answering these questions can help manufacturers establish a foundation and the pipelines needed to support secure development of IoT products. Secure development environments, pipelines, etc. are critical to ensuring efforts to produce securable IoT products are executable and effective. The development of securable products will employ additional activities targeted more directly at the conception and creating of the IoT product.

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

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

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

> *Customers* are the individuals or organizations who purchase and deploy an IoT product and will commonly act as administrators of the product for cybersecurity purposes, making use of product cybersecurity capabilities to help achieve their needs and goals. In addition to customers, some IoT products may have other *users* who did not purchase the equipment but nonetheless interact with the device or other IoT product components and may have cybersecurity needs and goals as well. Most customers are also users of the IoT products they

purchase, but not all IoT products have users in addition to the customer. The rest of this publication will refer to customers since every IoT product has a customer, but as discussed next, manufacturers should consider *how* a product may be used, including whether there may be users of the IoT product other than the customer.

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

1. **Who are the expected individuals to be customers or users for this product?** (e.g., musicians, small business owners, cyclists, police officers, chefs, home builders, preschoolers, electrical engineers, seniors, students)
2. **What types of organizations are expected to acquire this product?** (e.g., individual home users, small retail businesses, large hospitals, energy companies with solar farms, educational institutions with buses)

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

1. **How will the product be used?** (e.g., for a single purpose or for multiple purposes; embedded within another IoT product or not embedded, single user or customer or multiple users; private or commercial use)
2. **Where geographically will the product be used?** (e.g., countries, jurisdictions within countries)
3. **What physical environments will the product be used in?** (e.g., inside or outside; stationary or moving; public or private; movable or immovable; extreme or specific physical and weather conditions)
4. **What digital environments will the product be used in?** (e.g., unmanaged Wi-Fi networks; managed enterprise or industrial networks)
5. **How long is the product expected to be used?** (e.g., a few hours; several years; two decades)
6. **What IoT product components besides the IoT device will the product rely on to function?** (e.g., a backend; companion mobile or web application; or specialty networking/gateway hardware)
7. **What external dependencies on other systems will the product likely have?** (e.g., requires use of a particular third-party IoT hub or can integrate with third-party management applications)
8. **How might attackers misuse or compromise the product in the expected physical and digital environments?** (i.e., potential pairings of threats and vulnerabilities, such as in a

threat model including consideration of network connections that may provide a path to the internet that can be used as a vector of attack against other networks or devices)

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

Answers to these and similar questions can help the manufacturer establish their intended context for the IoT product (i.e., how, where, when, and by whom the product will be used). Note, a manufacturer can work to establish an *intended context*, but when IoT products are deployed in the post-market phase, customers have the ability to use the products they own in contexts as they see fit, which may not align with the manufacturer's intended context. Nonetheless, understanding intended context is critical to informing the design of a securable IoT product.

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.

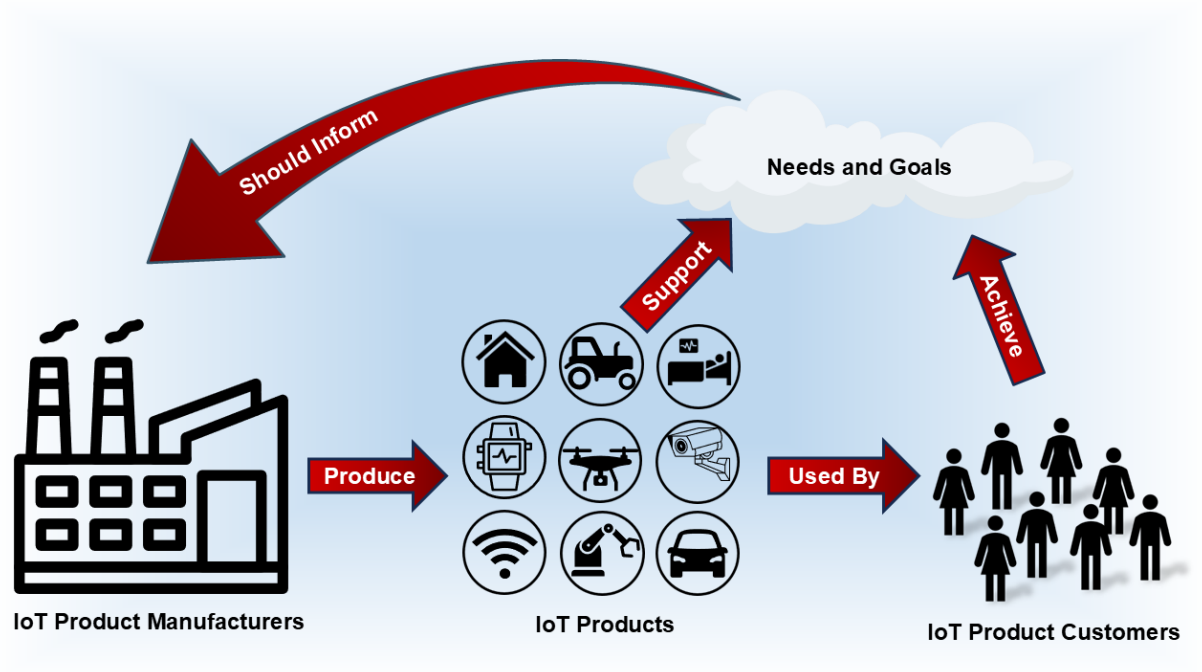

Figure 4. Cybersecurity connections between IoT product manufacturers and customers.

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?** Some IoT products, such as connected medical equipment, may provide critical non-IT-based functionality to customers. These IoT products may have operational characteristics that interfere with the customer's ability to use product cybersecurity capabilities. Other IoT products may be used in environments with characteristics (e.g., physical remoteness, harsh condition) that also hinder the application of cybersecurity capabilities..
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, aggregated, or modified by unauthorized entities, including potential human-safety and privacy implications. 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, create unexpected interdependencies among products, or cause unanticipated interactions and outcomes. This may, in turn, impact the operating

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

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

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

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

As Fig. 5 conceptually depicts, IoT product manufacturers can use a variety of sources to gather the information they need to answer these questions and others. In some instances, expected customers and use cases will point to existing laws, regulations, or voluntary cybersecurity or operational guidelines. For example, IoT products intended to be used by the federal government would be secured using controls derived from system cybersecurity guidelines that are required for federal agencies (e.g., NIST SP 800-53 [5], Cybersecurity Framework [8], NIST SPs 800-213 [20] and 800-213A [21]), which in some cases identify or imply specific product cybersecurity capabilities that an agency would need to support controls used in their system. For some use cases, guidance may go beyond cybersecurity risks but will still have direct or

indirect implications for cybersecurity, such as devices in the Healthcare and Public Health sector needing to comply with Food and Drug Administration (FDA) regulations and the Health Insurance Portability and Accountability Act (HIPAA). It is possible that in order to meet FDA recommendations and HIPAA requirements, an IoT product may need strict data confidentiality, integrity, and/or availability protections well beyond what is included in an average IoT product. By understanding these regulations in the context of the expected use cases, manufacturers can determine how to best support their customers' needs and goals. Many industrial sectors will also have consensus and/or voluntary guidelines (e.g., frameworks, baselines, and best practices) that should be followed by their stakeholders. In the healthcare context, one example of a voluntary consensus standard is *Health software and health IT systems safety, effectiveness and security Part 5-1: Security — Activities in the product life cycle*, IEC 810015-1, [22] while for industrial control system devices, manufacturers could look to *Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements*, ISA/IEC 62443-4-1. [23] Increasingly, geographic regions may have voluntary or mandatory IoT product cybersecurity programs, such as the Cyber Security Agency of Singapore's Cybersecurity Labelling Scheme or the European Union's Cyber Resilience Act.

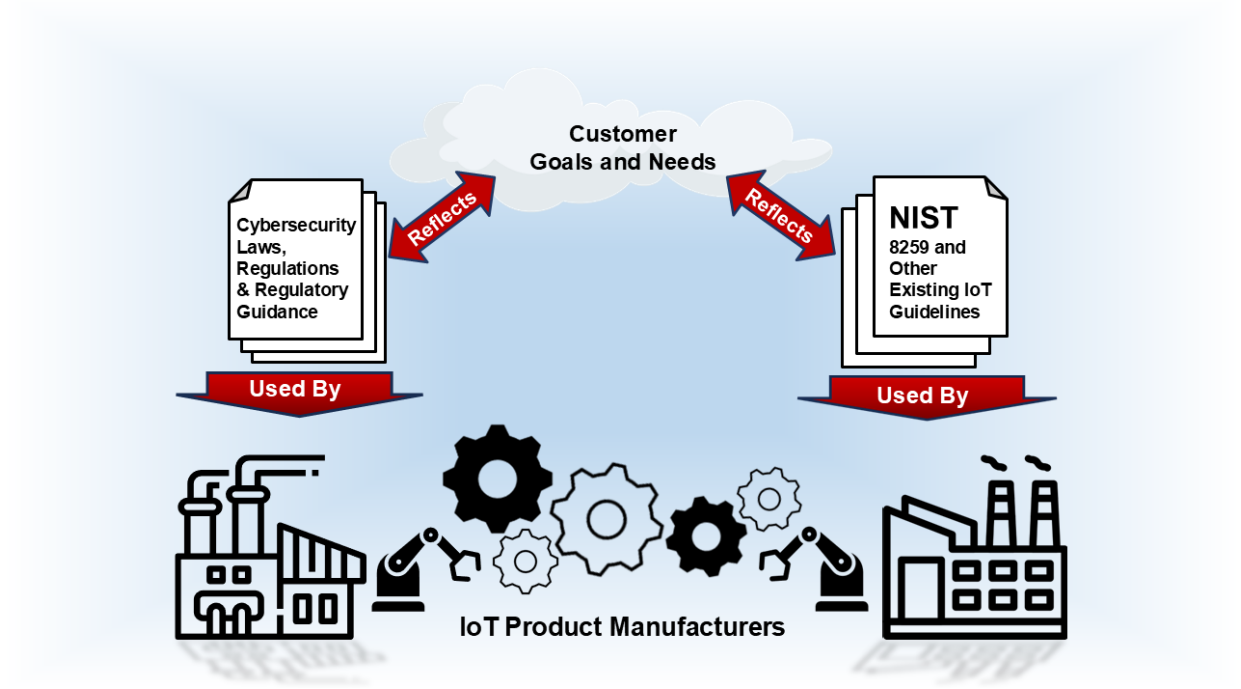

Figure 5. Customer cybersecurity needs and goals reflected in and informed by many applicable regulations and other documents.

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

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

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

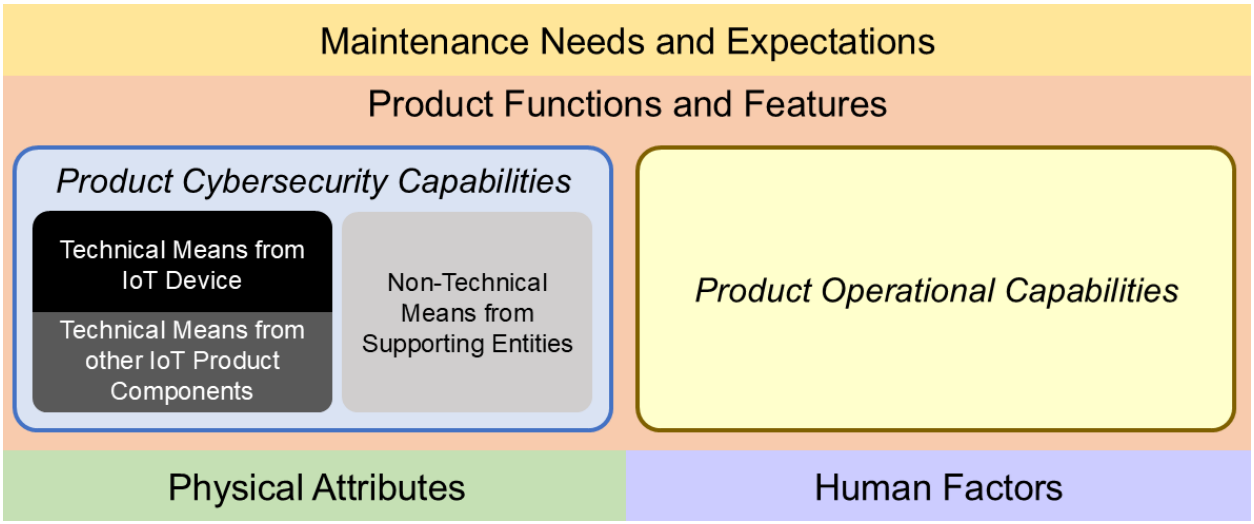

Figure 6. How other factors can build up to include, but not be limited to, the product cybersecurity capabilities composed of technical and non-technical means.

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

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

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

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

1. The IoT device can provide the technical means through its device cybersecurity capabilities (for example, by using device cybersecurity capabilities built into the device's operating system).
2. Another IoT product component can provide the technical means on behalf of the IoT device. This may include other systems and services that may or may not be acting on behalf of the manufacturer providing the technical means (e.g., a cloud-based service that securely stores data for each IoT product, internet service providers and other infrastructure providers).
3. In addition to and in support of technical means, non-technical means (e.g., communication of lifespan and support expectations, disclosure of flaw remediation plans) can also be provided by manufacturers or other organizations (i.e., supporting entities) and services acting on behalf of the manufacturer.
4. The customer can select and implement other technical and non-technical means for mitigating cybersecurity risks. The customer can also choose to respond to cybersecurity risks in other ways, including accepting or transferring the risk. For example, an IoT product may be intended for use in a customer facility with stringent physical security controls in place and thus may not support multi-factor authentication for access control to the IoT device component.

Note that there is not necessarily a one-to-one correspondence between needs or goals and means; for example, it may take multiple technical means to achieve a goal, and a single technical means may help address multiple goals. Additionally, not all needs and goals can or need to be addressed using only technical means, and some technical means themselves may require additional non-technical means for initial and on-going securability (e.g., knowledge of which product cybersecurity capabilities are available, ability to gather and apply software updates).

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

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

- Ecosystem obligations like applicable standards, laws, and regulations or contractual obligations the manufacturer may have with other entities.
- Physical product considerations such as size, shape, and weight which can limit or otherwise influence the selection of appropriate and applicable means for cybersecurity.
- IoT product lifecycle and maintenance expectations may impact the selection of means, especially those that require on-going support through the lifecycle or frequent maintenance.

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

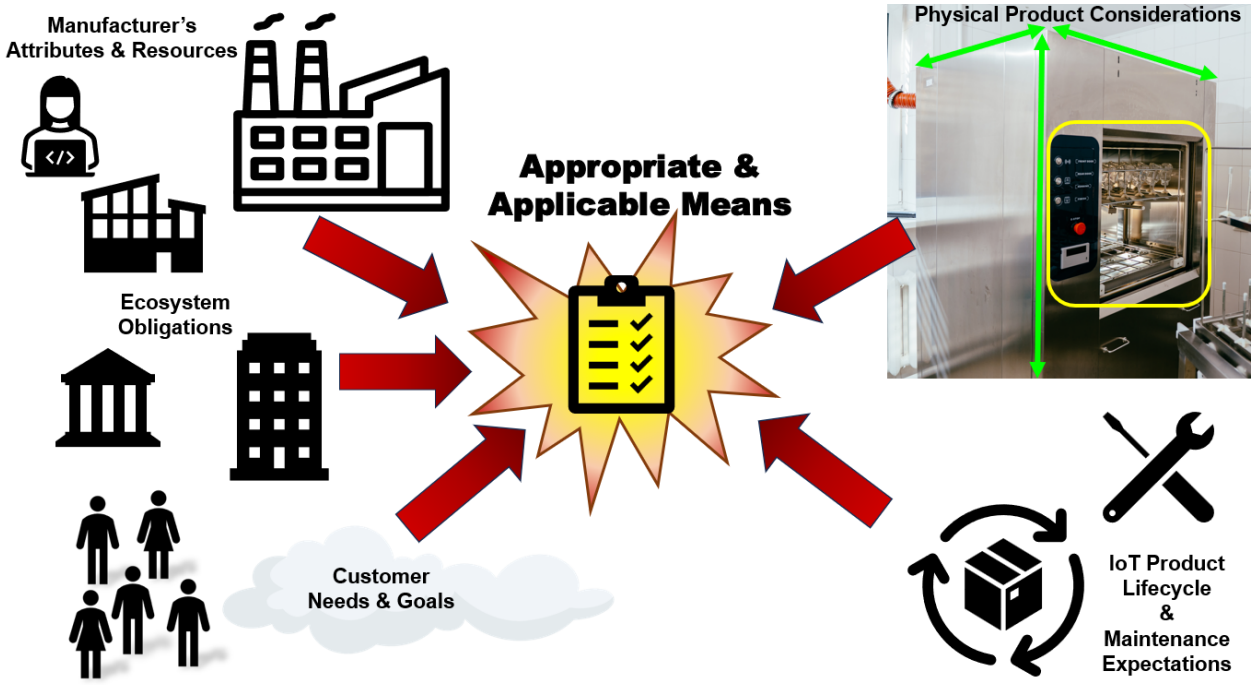

Figure 7. Various factors combine to influence appropriate and applicable means for cybersecurity.

IoT manufacturers could use an understanding of means to document and express cybersecurity support they aim to provide for their IoT product. Organizing technical and non-technical means and using them to define product cybersecurity capabilities can enable a broader view of cybersecurity throughout the IoT product's lifecycle and easier communication 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 needed by the expected customers. 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 needs to provide should happen as early as feasible in the product design processes so the capabilities can be considered when selecting or designing IoT product hardware and software. To provide manufacturers a starting point in identifying the necessary device cybersecurity capabilities for their IoT devices, a companion publication the IoT Device Cybersecurity

Capability Core Baseline, NISTIR 8259A defines a device cybersecurity capability core baseline,[4] which is a set of device capabilities generally needed to support common cybersecurity controls that protect the customer's devices and device data, systems, and ecosystems. The device cybersecurity capability core baseline has been derived from common cybersecurity risk management approaches. The core baseline is just one set of product cybersecurity capabilities that may be needed in an IoT product, and manufacturers should consult other sources to identify appropriate product cybersecurity capabilities for expected customers and use cases.

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

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

Additional baselines of IoT product cybersecurity capabilities may exist from NIST or other organizations, some of which may be designed to address the needs of particular customer groups, industrial sectors, use cases, etc. For example, NIST has published *Profile of the IoT Core Baseline for Consumer IoT Products*, NISTIR 8425 [24] and *IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog*, SP 800-213A [21]. These resources can help manufacturers identify necessary product and device cybersecurity capabilities for the context in which their IoT device will be used.

Since product cybersecurity capabilities will be shaped by the context of the customer and use case, different IoT products will need different *sets* of product cybersecurity capabilities. Though useful as a starting point, the high level of the device cybersecurity capability core baseline means that it will need to be profiled for specific IoT products based on the needs and goals of the expected use case. Product cybersecurity capabilities drawn from the core baseline

[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.

or other high-level sources can be profiled and built upon in a variety of ways. New or more complex capabilities may be required in a product. High-level product cybersecurity capabilities can be expanded and adapted in ways that better align with what specific customers need or prefer (e.g., product cybersecurity capabilities adapted for the federal government [21]).

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

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

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

1. **Considering expected terms of support and lifespan, what potential future use needs to be taken into account?** For example, if a product has a 10-year lifespan, it may be necessary to update the encryption algorithm or key length the product uses during that time, and the new algorithm or key length may require more processing resources than is currently provided. Consider how the product can support cybersecurity needs and goals for the product's lifespan, including "future proofing" of the product cybersecurity capabilities and their implementations. For example, when considering encryption modules, the selection of quantum-safe approaches (See [25] [26] [27]) can help "future proof" the securability of the IoT product. As an IoT product moves deeper into its lifespan, the ability for customers to determine the support status for products is important to making products securable.
2. **Should an established IoT platform be used instead of acquiring and integrating individual hardware and software components?** An *IoT platform* is a piece of hardware or supporting software upon which a new IoT product can be created. IoT platforms may have some IoT product components or capabilities already installed and configured for a manufacturer's use. An IoT platform might also offer various configuration capabilities, third-party services or applications, or a software development kit (SDK). Manufacturers can choose a sufficiently resourced and adequately secure IoT platform to reduce some or all of the cybersecurity risks associated with designing hardware, installing and configuring an

operating system, creating new cloud-based services, writing IoT product component applications and mobile apps from scratch, and performing other tasks that are error-prone.

3. **Should any of the product's, especially the device's, cybersecurity capabilities be hardware-based or bound cryptographically?** An example is having a hardware root of trust that provides trusted storage for cryptographic keys and enables performing a secure boot and confirming the IoT product and device authenticity. An additional example is the establishment of an identifier bound to the IoT product cryptographically. Further, manufacturers should consider whether those hardware-based capabilities will be updatable, such as to facilitate a move to post-quantum cryptography when possible. For example, in some cases, customers will need an immutable hardware root of trust and never want updates or changes to that functionality, but such limitations could be detrimental to ongoing securability for other customers.
4. **Does the hardware or software (including the operating system) include unneeded product capabilities with cybersecurity implications? If so, can they be disabled to prevent misuse and exploitation?** For example, an IoT device may have local interfaces on its external housing that are essential for some current, or future expected, use cases. But if the device may be deployed in public areas, those interfaces would be exposed to possible attack. Possible approaches to this issue include offering a tamper-resistant enclosure to prevent physical access to the interfaces or providing a configuration option that logically disables the interfaces.
5. **Will the IoT product employ components based on artificial intelligence or use automated decision-making in its operation? If so, what transparency or safeguards are appropriate to ensure the confidentiality, integrity, or availability of the IoT product's data and operation?** For example, an IoT product may have operational characteristics that are relied upon by a customer for mission critical applications, and so their knowing that the IoT product has certain artificial intelligence-power components or features can help the customer adequately control the risks faced by the IoT product.

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

1. **Which product cybersecurity capabilities are relevant to each IoT product component?** Manufacturers often design IoT products leveraging multiple IoT product components in ways that allow each component developer to specialize in actions for which they are best suited. For example, backends generally have near limitless storage and substantial processing capabilities, whereas companion applications have the benefit of access to the customer and mature, standardized interface capabilities. How an IoT product component

fits into the IoT product's operations can impact the threats and risks that particular IoT product component faces and how those risks might be mitigated.

2. **How can each relevant product cybersecurity capability be appropriately implemented for each IoT product component?** For example, a backend is generally inaccessible to customers; customer-facing product cybersecurity capabilities (e.g., asset identification for use by the customer) may be irrelevant. Other product cybersecurity capabilities (e.g., software update capabilities for companion applications) may be supported differently, taking advantage of update capabilities provided by the operating system or other platform they run on. Still other product cybersecurity capabilities (e.g., protection of data at rest and in transit) may be implemented similarly across all IoT product components.
3. **How can cybersecurity be supported within the IoT product boundary?** It is important to consider that an IoT product comprised of multiple IoT product components is a system, and cybersecurity protections within the boundary of the IoT product can utilize system cybersecurity techniques even if their customers do not expect them or use them. For example, cybersecurity within the IoT product boundary could be supported by implementation of a Zero-Trust Architecture.
4. **How much control and cybersecurity responsibility will the customers, manufacturer, or other entities have over each IoT product component?** Cybersecurity in the context of IoT products will require some amount of coordination between manufacturers and customers and may involve other entities (e.g., installers, integrators). Manufacturers should consider how the IoT product can best support each of these entities throughout the product's lifecycle. This support will vary depending on how much control each entity has over cybersecurity and how much cybersecurity responsibility each entity has. For example, cybersecurity state data should be available from IoT products to support customers' digital forensics investigations, but acquiring the data may require the involvement of the product manufacturer or 3rd parties. Refer to Section 3 of this document for a discussion of these considerations.
5. **How can necessary cybersecurity support be coordinated for all IoT product components, potentially across multiple entities?** Coordination between entities can take many forms. Expected technical product cybersecurity capabilities being present in equipment affords securability and allows entities to use the product securely. Sometimes coordination requires non-technical interactions, particularly if visibility into technology or organizations is limited. For example, backends can be hosted by third-parties that the manufacturer does not have insight into, necessitating the setting and enforcement of cybersecurity expectations through means such as business-to-business dialogue and contracts. For IoT products generally, there will be required interactions between manufacturers and customers. For example, since a manufacturer cannot anticipate all potential customers and users, they may rely on non-technical means such as disclaimers and warning messages to communicate key cybersecurity considerations in a way accessible to as many potential customers and users as possible. Even for customers and users that the manufacturer can anticipate, the complexities of deployment, installation, and use of IoT products may require non-technical cybersecurity support such as detailed lists of answers to frequently

asked questions or text and video tutorials guiding customers and users in securely using the IoT product.

Manufacturers should consider which secure development practices[5] and other non-technical supporting capabilities are most appropriate in planning how to adequately support customer needs and goals. Manufacturers can answer questions like the following based on expected 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, perform red-teaming exercises, penetration testing, and jailbreak testing on the IoT product and its product components)
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, coordinated vulnerability disclosures, 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

[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.

inventories all end-points automatically, machine-readable cybersecurity disclosures and support-status feeds)

9. **Are there aspects of the IoT product that have non-cybersecurity risk considerations for which related frameworks or tools are available?** (e.g., machine learning, automated decision-making, and other forms of artificial intelligence that could be informed by the NIST AI Risk Management Framework [28], collection and processing of personal data that could be informed by the NIST Privacy Framework [29], use of digital identities that could be informed by *Digital Identity Guidelines*, NIST SP 800-63 Rev. 4 [30])

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

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

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

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

4.1. Activity 6: On-Going Support of Product Cybersecurity throughout the Lifecycle and through End-of-Life

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

1. **What is the IoT product's intended operational, and thus cybersecurity, context?** Variance in deployment conditions may void manufacturer cybersecurity assumptions that should be addressed by those individuals or organizations deploying an IoT product. For example, a network-connected water valve may be intended to be used in commercial plumbing applications and not in the critical infrastructure context. If the valve were deployed in a water/waste-water facility, additional cybersecurity controls may be needed than was assumed for the commercial context.
2. **Which ecosystem entities have cybersecurity responsibilities related to the IoT product when deployed?** Cybersecurity often necessitates direct or indirect collaboration between various individuals and organizations. For example, most of this publication highlights the critical cybersecurity role manufacturers have via their development of IoT products, but this is not where cybersecurity ends. The individuals or organizations that use, deploy, maintain, support, etc. the IoT product can also have a role in cybersecurity, and manufacturers, in their role as developers of the IoT products, can help in the post-market phase by clarifying cybersecurity roles and responsibilities.
3. **Which product cybersecurity capabilities *require* post-market cybersecurity support?** Product cybersecurity capabilities may need to be updated over time. For example, digital asset identifiers may be upgraded to accommodate more unique values as a product base grows. Software updates will also be deployed post-market, which will be critical to keeping IoT products in service longer and minimizing open vulnerabilities across the internet.
4. **Which product cybersecurity capabilities *enable* post-market cybersecurity support?** Some product cybersecurity capabilities may be important to enabling post-market cybersecurity support. Considering the prior example of updating a digital asset identifier, software update capabilities could be used to achieve these updates. Non-technical cybersecurity capabilities (e.g., Information and Query Reception and Information Dissemination documented in NIST IR 8259B [11]) are critical to facilitating post-market cybersecurity support.
5. **How can all ecosystem entities be proactive in identifying and mitigating emerging cybersecurity threats and risks?** During the post-market phase, manufacturers are not alone in ensuring the cybersecurity of the IoT product. They may have a role in ensuring on-going securability of the product, but so may other ecosystem entities. There may be various actions participants in this ecosystem can take to ensure threats are visible and risks are mitigated, for example:
    - IoT product manufacturers can prioritize actions on vulnerability and bug reports from the public by making software updates to remediate the issues.
    - Integrators can maintain awareness of known issues with IoT products they have installed for customers and work with customers to minimize the risks.
    - Customers can seek support information for their IoT products, ensure the most up-to-date software is installed, and plot next steps if products are out of their support period and are no longer receiving updates.

6. **As cybersecurity and other digital support for the IoT product ends, what actions will the manufacturer take to ensure the products remain securable?** IoT products may remain in service much longer than software or other digital components are supported or state-of-the-art. Unsupported or deprecated digital equipment used in the field is sometimes called "legacy." Though legacy IT equipment is an issue for some sectors, legacy IoT products are relatively common, especially for industrial applications. Unmanaged environments, (e.g., homes and small businesses) can also accumulate legacy IoT products. Use of legacy products is not natively a cybersecurity issue, but legacy products have significantly higher likelihood of the presence of and easy exploitation of vulnerabilities in software or hardware. Mitigation of these vulnerabilities may be possible but could prove challenging due to required coordination with customers, who may be difficult to contact and motivate. Manufacturers can minimize the impact of support ending for their IoT products by engaging with customers while also ensuring the final updates maximize on-going securability of the IoT product. For example, if remote IoT product components (e.g., a backend) are to be removed when support ends, some or all of the product cybersecurity capabilities delivered by the backend can be migrated to other IoT product components.
7. **As the IoT product approaches the end of its useful life (i.e., end-of-life), how can the product remain securable?** For some IoT products (e.g., large equipment like vehicles and appliances), their useful life may far surpass that of the digital technologies the product uses (i.e., the product may have an extended legacy period). Legacy considerations highlighted in the previous question related to end-of-support are amplified in this extended legacy situation, so there may be justification to minimize, or remove entirely, networking capabilities that provide the IoT product broader internet access.
8. **When an IoT product is no longer securable, how can it be securely decommissioned and disposed of?** Even when used as legacy products, all IoT products will eventually no longer be useful. This may be because the use case for the product no longer exists or because the product has failed components that keep it from fulfilling its operational functions. Thus, all products will eventually need to be fully decommissioned and disposed of in a manner that preserves the cybersecurity of the product's customers and users. Disposal considerations are key here since customers will seek to remove or replace these products, which may have cybersecurity implications. For example, how can data be protected from unauthorized access after the disposed IoT product leaves the customer's control and possession.

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

4.2. Activity 7: Define Approaches for Communicating to Customers

For most IoT products and post-market cybersecurity support plans, communication with customers and other entities within the IoT product's ecosystem is foundational. Clearly

communicating cybersecurity information may necessitate different communication approaches for different kinds of customers based on their expectations and resources. Manufacturers can answer questions like the following to help define communication approaches:

1. **What is the purpose of the communication?** Communicating cybersecurity information places demands on both the manufacturer and customer. The manufacturer must prepare and effectively deliver the message while customers must expend time and effort to understand and decide how to use the information. As such, cybersecurity communications should be focused on key disclosures or calls for action to customers.
2. **What terminology will the customer understand?** A home user will likely have less technical knowledge than points of contact at a large business (e.g., system administrators). For example, IT and cybersecurity professionals may already be familiar with conventions like referring to a vulnerability by its Common Vulnerabilities and Exposures (CVE) number while home users likely will not.
3. **How much information will the customer need?** Giving some customers too much information may overwhelm them and make it harder for them to find the information they need. Not providing enough information is generally undesirable, except for cases where revealing the information might have broader negative implications—for example, publishing technical details of a newly discovered vulnerability before an update is available to correct the vulnerability.
4. **Which disclosures should be human-readable and which should be machine-readable?** Depending on various factors, including the customer or supporting entities' ability to consume them, some cybersecurity disclosures can be made in machine-readable format. This can support customers who take advantage of machine-readability to automate parts of the chain that handles cybersecurity disclosures.
5. **How/where will the information be provided?** Information can be provided in one or more logical and/or physical locations. Examples include user manuals, terms of service and other product documentation, websites, emails, and the IoT product components themselves (e.g., mobile apps). Customers will benefit more when they can readily locate information whenever needed.
6. **How can the integrity of the information be verified?** For some methods of providing information, such as emails, customers may want a way to determine if the information is legitimate (e.g., not a social engineering attempt).
7. **Will customers need to communicate with the manufacturer?** For example, customers may seek out updates or other data needed for maintaining their products, including servicing the IoT device. Customers may also discover vulnerabilities or other issues that they want to report. The functionality, usability, and efficacy of the communication channels from customer to manufacturer should be tested by the manufacturer to ensure customers and others (e.g., security researchers) can make use of the channels.

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

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

4.3.1. Cybersecurity Risk-Related Assumptions

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

1. **Who were the expected customers?** Some IoT products are created with a specific sector or customer type in mind, which could impact not only which product cybersecurity capabilities are implemented, but also how those capabilities function.
2. **How was the product intended to be used?** Some IoT products have specific intended purposes when deployed, which can help scope the cybersecurity customers may expect from the product. Additionally, some IoT products are expected to be used in particular systems, possibly creating cybersecurity dependencies that customers need to know about (e.g., a device requires a monitoring system to be able to connect to it for cybersecurity purposes).
3. **What types of environments would the product be used in?** Customers may need to know, for example, if an IoT product may not be securable in a public location or without the use of another device or specific application that provides some or all product cybersecurity capabilities on behalf of the IoT product. Network bandwidth and latency, as well as other environmental factors, may also impact which capabilities to incorporate and how to implement them.
4. **How would responsibilities be shared among the manufacturer, the customer, and others within the IoT product's ecosystem?** Some customers may benefit from knowing if implementation of product cybersecurity capabilities and related tasks (e.g., software updates, product configuration, data protection and destruction, and product management) are the responsibility of one party or multiple parties.

4.3.2. Support and Lifespan Expectations

Communicating product support and lifespan expectations helps customers plan their cybersecurity risk mitigations throughout the product's support lifecycle, which may be shorter than how long the customer wants to use the product. Recall that as discussed in Activity 2, manufacturers may have identified regulatory requirements that might require notification a minimum length of time in advance of end of support or specify minimum requirements for support from time of purchase, but even absent regulation, communication of product support

and lifespan expectations is beneficial for cybersecurity. To determine what information to communicate to customers, manufacturers can answer questions like the following:

1. **How long is support for the product intended to be provided?** Telling customers how long updates and technical support will be available may help them plan to securely use and maintain products for an appropriate amount of time.
2. **When is it intended for product end-of-life to occur? What will be the process for end-of-life?** Customers may want to retire a product, or at least change how the product is used, when the manufacturer considers the product and its device component at end-of-life. These customers may benefit from advance notice (e.g., six months) leading up to that end-of-life so that they can plan for the event. In some cases, other entities may be the primary recipient of end-of-life notification. For example, a registry or consortium of registries could be established to track when products are designated as "end-of-life" by their manufacturers or such a designation is driven by events (e.g., manufacturer goes out of business and ceases to exist). Such registries could be the entity informed by manufactures of when their IoT product is no longer supported, and customers can look to the registries when researching or maintaining products.
3. **What functionality, if any, will the product have after support ends and at end-of-life?** Customers may want to know if they will be able to continue use of a product at its end-of-life, even if cloud-based services or other functions are no longer available. (i.e., will a freezer continue to function as a freezer even if automatic inventorying applications are not available)
4. **How can customers report suspected problems with cybersecurity implications, such as software vulnerabilities, to the manufacturer? Will reports be accepted after support ends? Will reports be accepted after end-of-life? Will any action be taken with these reports (e.g., posting to a website) after support ends?** Examples of reporting methods include phone numbers, email addresses, and web forms.
5. **How can customers maintain securability even after official support for the product has ended (e.g., when a manufacturer or third-party organization with a cybersecurity role shuts down entirely or ends support of the product)? Will essential files or data be made available in a public forum to allow others, even the customers themselves, to continue to support the IoT product?** For example, a manufacturer going out of business may make the code base of their product available in an open-source repository to allow continued development and support from the community.

4.3.3. Product Composition and Capabilities

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

1. **What information do customers need on general cybersecurity-related aspects of the product, including installation, configuration (e.g., hardening guide), usage, management, maintenance, and disposal?** Examples include how the product can securely join a system or network, which configuration options may impact cybersecurity and how they may impact it, and what ways of using the product are known to be insecure.
2. **What is the potential effect on the product if the cybersecurity configuration is made more restrictive than the default?** Some products may lose some functionality as their cybersecurity configurations are made more stringent.
3. **What inventory-related information do customers need related to the product's internal software, such as versions, patch status, and known vulnerabilities?** Do customers need to be able to access the current inventory on demand? Some customers may want to be aware of known vulnerabilities so they can address them, while other customers may want to know current software patch status.
4. **What information do customers need about the sources of the product's software, hardware, and services?** Examples of sources include the developer of the product's software, the manufacturer of the device's processor, and the provider of a cloud-based service used by the product. Techniques such as a software bill of materials (SBOM) and hardware bill of materials (HBOM) can be considered as a way to communicate this and similar information to customers consistently and effectively.
5. **What information do customers need on the product's operational characteristics so they can adequately secure the product?** How should this information be made available? Some customers may be best served by placing the information on a website, while others may make best use of the information through a standardized machine-to-machine protocol. In some cases, such as for device intent signaling, this information or links to it might be best provided through the product itself.
6. **What functions can the product perform?** This includes not only product cybersecurity capabilities, but also any other functions that may have cybersecurity implications—for example, transmitting data to a remote system, or using a microphone and camera to capture audio and video.
7. **What data types can the product collect?** What are the identities of all parties (including the manufacturer) that can access that data? Some customers may need to know if location information or voice commands collected by the product may be stored in a cloud and accessed for other purposes, possibly by other parties (e.g., for aggregation or analytics).
8. **What kind of post-processing of the data is performed by entities, both as part of the product's operation and as part of the manufacturer's or other entities' systems?** For example, a video camera may send data to a backend, where it is processed for motion so that clips of the motion or other notifications can be made available to the customer. Outside of the context of the product's operation, the data may also be processed for the purpose of informing advertising profiles of the customer. Informing customers about how their data is post-processed can help them adequately plan effective cybersecurity controls by helping them understand the full digital operational context.

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

4.3.4. Software Updates

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

1. **Will updates be made available? If so, when will they be released?** Knowing if updates will be provided on a set schedule or sporadically will help customers plan for applying them.
2. **Under what circumstances will updates be issued?** Examples include controlling the execution of faulty software and correcting a previously unknown vulnerability in a standard protocol.
3. **How will updates be made available or delivered? Will there be notifications when updates are available or applied?** Customers can better plan for applying updates if they know they must be downloaded through a specific portal and applied to the device. Customers may also benefit from being notified that an update has to be or has been applied, even in cases where the delivery and application of the software update is automatic, over-the-air, and requires no action from the customer or users.
4. **Which entity (e.g., customer, manufacturer, maintainer) is responsible for performing updates? Or can the customer designate which entity will be responsible (e.g., automatically applied by the manufacturer)? Do responsibilities vary for different IoT product components?** Some customers may benefit from knowing that certain IoT device updates will be available from a third party and that other updates will be provided by the manufacturer. Some customers may likewise benefit from being made aware of their roles, responsibilities, and options regarding updates. This will likely vary for different IoT product components. For example, IoT devices may be managed by customers in many cases, but most backends will not.
5. **How can customers verify and authenticate updates? Can verification and authentication of updates be achieved automatically by the IoT product?** Examples are cryptographic hash comparison, code signature validation, and reliance on manufacturer-provided software that automatically performs update verification and authentication.
6. **What information should be communicated with each individual update?** Examples include the reason for the update (e.g., corrections to errors, altered or new capabilities) and any effect installing the update could have on a customer's existing configuration settings.

4.3.5. Product Retirement Options

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

1. **Will customers want to transfer ownership of their IoT products to another party? If so, what do customers need to do so their user and configuration data on the IoT product are not accessible by the party who assumes ownership?** For example, a customer may want to sell a facility that contains smart building automation devices and would want a way to ensure all data has been removed from the devices before the buyer gains access to them.
2. **Will customers want to render their devices inoperable? If** so, how can customers do that? Some IoT devices can be rendered inoperable through logical means (e.g., as executed through a mobile app), while others use physical means (e.g., a button on the device).

4.3.6. Technical and Non-Technical Cybersecurity Capabilities

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

1. **Which product cybersecurity capabilities can be provided:**
    a. **by the device itself (device cybersecurity capabilities)?** Examples include encryption used by the device for data protection, the presence of a physical identifier on the device, and authentication and authorization mechanisms the device uses to limit access to its network interfaces.
    b. **by other local product components?** Some technical means may be delivered or supported by an IoT hub or mobile app that is part of the IoT product.
    c. **by a manufacturer service, system or other remote product components?** An example would be technical means provided by an internet server or cloud-hosted service.
2. **Which non-technical means can be provided by the manufacturer or other organizations and services acting on behalf of the manufacturer?** Examples include many of the concepts discussed throughout this section, such as lifespan expectation, software update plans, and retirement options. In addition to those discussed in this section, there may also be other non-technical means (e.g., how a flaw or vulnerability may be reported) customers would benefit from knowing about and understanding.
3. **Which technical or non-technical means should the customer provide themselves or consider providing themselves?** Examples would be using network-based security controls (e.g., a firewall) to prevent direct access to local IoT product components from the internet

and performing audits of the implementation and settings to ensure compliance requirements are met.

4. **How is each of the technical and non-technical means expected to affect cybersecurity risks?** For example, proper implementation of data protection may help mitigate confidentiality risks, but may also reduce availability (e.g., if data cannot be decrypted or is decrypted slowly).
5. **How do product cybersecurity capabilities support security controls in the deployed environment?** For example, customers can benefit from a mapping between the product cybersecurity capabilities offered by the IoT product and organizational cybersecurity controls reflected in guidance documents.

5. Conclusion

This publication discusses nine cybersecurity-related activities for IoT product manufacturers and gives examples of questions manufacturers can answer for each activity. Manufacturers who choose to perform one or more of these foundational cybersecurity activities should determine the applicability of the example questions and identify any other questions that may help to understand customers' cybersecurity needs and goals, including the product cybersecurity capabilities their customers expect. The questions highlighted for each activity are meant as a starting point and do not entirely define each activity. Also, the process described in this publication is not meant to imply that the role of manufacturers is limited to providing capabilities that require action by customers, but rather should drive manufacturers to better understand their customers' needs and goals in the context of the IoT product, which may require automated capabilities, and/or additional supporting non-technical actions. For some customers and use cases, where it is possible and appropriate, limited customer responsibility for cybersecurity may lead to better cybersecurity outcomes for the ecosystems 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 IoT of Things Oct 2024 508 FINAL_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 KA, Pease M, Tang CY, Zimmerman T, Pillitteri VY, Lightman S, Hahn A, Saravia S, Sherule A, Thompson M (2023) Guide to Operational Technology (OT) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-82r3. https://doi.org/10.6028/NIST.SP.800-82r3

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

[14] Quinn SD, Chua J, Ivy N, Gardner RK, Kent K, Smith MC, Witte GA (2025) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8286r1. https://doi.org/10.6028/NIST.IR.8286r1

[15] Quinn S, Ivy N, Chua J, Barrett M, Feldman L, Topper D, Witte G, Gardner RK, Scarfone K (2023) Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-221. https://doi.org/10.6028/NIST.SP.800-221

[16] Quinn S, Ivy N, Chua J, Scarfone K, Barrett M, Feldman L, Topper D, Witte G, Gardner RK (2023) Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-221A. https://doi.org/10.6028/NIST.SP.800-221A

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

[18] Souppaya M, Scarfone K, Dodson D (2022) Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-218. https://doi.org/10.6028/NIST.SP.800-218

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

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

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

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

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

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

[25] National Institute of Standards and Technology (2024) Module-Lattice-Based Key-Encapsulation Mechanism Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 203. https://doi.org/10.6028/NIST.FIPS.203

[26] National Institute of Standards and Technology (2024) Module-Lattice-Based Digital Signature Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 204. https://doi.org/10.6028/NIST.FIPS.204

[27] National Institute of Standards and Technology (2024) Stateless Hash-Based Digital Signature Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 205. https://doi.org/10.6028/NIST.FIPS.205

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

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

[30] Temoshok D, Proud-Madruga D, Choong Y-Y, Galluzzo R, Gupta S, LaSalle C, Lefkovitz NB, Regenscheid AR (2025) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63-4. 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

USB
Universal Serial Bus

UWB
Ultra-Wideband

Wi-Fi
Wireless Fidelity

Appendix B. Glossary

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

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

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

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

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

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

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

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

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

Means
An agent, tool, device, measure, plan, or policy for accomplishing or furthering a purpose. [17] In the context of this publication, we discuss technical means, which come from hardware and software, as well as non-technical means, which come from actions and procedures.

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

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

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

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

Transducer
A portion of an IoT device capable of interacting directly with a physical entity of interest. The two types of 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:
    - Within Section 2.2 **Composition of IoT Products**
        - Ending paragraphs and large callout box on IoT products' technical means discussion was removed.
    - 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.
    - 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)
    - 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.

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

- Within Section 3, changed the following:
  - Added "Activity 0: Prioritize Cybersecurity and Maintain Cybersecurity Posture" to clarify that manufacturing organizations need cybersecurity to be a focus of the product development process. This activity is added because it's been assumed implicitly this activity 0 has been taken by manufacturers to prioritize and maintain their organizational cybersecurity posture. And some organizations may have limited cybersecurity experience for a variety of reasons.
  - **Updates to** questions beginning that cybersecurity risk discussion (1-5 sourced from CSF):
    - Highlighting manufacturers can utilize tools such as the MITRE ATT&CK or EMB3D Frameworks to identify applicable threats.
    - Focusing on how the organization assess and mitigate cybersecurity risks by adding Added context that it's critical that IoT product manufactures aim for a strong cybersecurity posture with an indication that standards and tools exist to aid and references CSF, RMF and ISA/IEC 62443 [23].
  - Added considerations for developers and manufacturers and references for Secure Software Development Framework and NIST SP 800-161 rev 1 on supply chain risk management.
  - Closing paragraph indicating the rest of the activities concern the cybersecurity of IoT products rather than the cybersecurity posture of IoT manufacturers. This allows focus on the cybersecurity of their customers.
  - Within Section 3.2 **Activity 1: Identify Expected Customers and Define Expected Use Cases**, the following were updated:
    - First sentence added to clarify that Manufacturers should look to many sources for determining their IoT product requirements but one key source is the customer's needs and goals.
    - Defining requirements was removed.
  - Within Section 3.3**. Activity 2: Research Customer Cybersecurity Needs and Goals**
    - The callout box referencing Fig 4 was removed.

- The figure 4 title was updated – Cybersecurity Connections between IoT product manufacturers and customers.
- Paragraph was added in the to clarify the purpose of the questions.
- Following the paragraph on FDA/HIPAA – example voluntary consensus standards and international schemes were added including:
  - Healthcare: Part 5-1: Security — Activities in the product life cycle, IEC 810015-1 [22].
  - Industrial: Part 4-1: Secure product development lifecycle requirements, ISA/IEC 62443-4-1 [23].
  - Cyber Security Agency of Singapore's Cybersecurity Labelling Scheme or the European Union's Cyber Resilience Act.
  - Fig 5. Text updated.

- 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.
- 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:
  - 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.
  - 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.
  - 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.
  - 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).

  - Added description to Fig 7 'Various factors combine to influence appropriate and applicable means for cybersecurity' which illustrates how factors collide to shape an IoT product's technical and non-technical means for cybersecurity.
  - Added a paragraph following Fig 7 on: Manufacturers could use an understanding of means to document and express cybersecurity support aim to provide for the product. This can enable a broader view of cybersecurity through the product's lifecycle and better communication about cybersecurity features with ecosystem entities.
- Within Section 3.5 **Activity 4 - Define IoT Product Cybersecurity Capabilities Based on Appropriate Means,** figure was removed and moved to Section 2.
- Within 3.6 Activity 5: Plan for Adequate Support of Customer Needs and Goals, the following were updated:
  - Greater discussion of how IoT product manufacturers should consider that their decisions can have impacts on secureability and that they should make decisions to support all stags of IoT product's lifecycle
  - An example on post-quantum cryptography was added to question 3.
  - A new question and context were added to address new areas and risk considerations such as the inclusion of AI.

- Within Section 4, there were the following updates:
  - Within Section 4.1 **Activity 6: On-Going Support of Product Cybersecurity through-out the Lifecycle and through End-of-Life**, the following were updated:
    - The activity title was updated.
    - Question 5 was clarified by removing the final portion and creating a new question 6.
    - Additional context was added to question 6, to further expand on decommissioning and disposal.
  - Within Section 4.3.2 **Support and Lifespan Expectations**, the following were updated:
    - Question 2 was updated with a new discussion around different options at "end of life" of the product. The new paragraph discusses notifications, registries and related information.

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