Draft NISTIR 8259

Core Cybersecurity Feature Baseline for Securable IoT Devices:

A Starting Point for IoT Device Manufacturers

Michael Fagan
Katerina N. Megas
Karen Scarfone
Matthew Smith

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

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NISTIR 8259

Core Cybersecurity Feature Baseline for Securable IoT Devices:

A Starting Point for IoT Device Manufacturers

Michael Fagan
Katerina N. Megas
Applied Cybersecurity Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

Matthew Smith
G2, Inc.
Annapolis Junction, MD

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

July 2019

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

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

National Institute of Standards and Technology Interagency or Internal Report 8259
38 pages (July 2019)

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

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

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

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

Public comment period: July 31, 2019 through September 30, 2019

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

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

Reports on Computer Systems Technology

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

Abstract

This publication is intended to help Internet of Things (IoT) device manufacturers understand the cybersecurity risks their customers face so IoT devices can provide cybersecurity features that make them at least minimally securable by the individuals and organizations who acquire and use them. The publication defines a core baseline of cybersecurity features that manufacturers may voluntarily adopt for IoT devices they produce. The core baseline addresses general cybersecurity risks faced by a generic customer. Manufacturers often know more about their customers and the risks they face, so the publication also provides information on how manufacturers can identify features beyond the core baseline most appropriate for their customers and implement those features to further improve how securable their IoT devices are. This approach can help lessen the cybersecurity-related efforts needed by IoT device customers, which in turn should reduce the prevalence and severity of IoT device compromises and the attacks performed using compromised IoT devices.

Keywords

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

Acknowledgments

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

Audience

The main audience for this publication is IoT device manufacturers seeking a better understanding of how to identify the appropriate cybersecurity features for their IoT devices, or wanting a common language for communicating with others regarding these features. A secondary audience for this publication is IoT device customers (i.e., individuals and organizations) that want to specify which cybersecurity features they need from IoT devices during their evaluation and acquisition processes.

Note to Reviewers

NIST welcomes feedback on any part of the publication, but there is particular interest in the following:

1. Section 3 is intended to help IoT device manufacturers better identify the cybersecurity risks their expected customers (individuals and organizations) are likely to face, instead of assuming a generic set of risks faced by a generic set of customers. This would help manufacturers identify the cybersecurity features their customers need their IoT devices to have. Is the proposed process for identifying features appropriate and reasonable? If not, how can it be improved?
2. Are the cybersecurity features and the key elements of those features defined in Section 4 the right set for a generic starting point for IoT devices? If not, which cybersecurity features and key elements should be added, removed, or changed, and why?
3. We have received considerable feedback that the lack of transparency into the characteristics of many IoT devices can make it harder to understand and address the cybersecurity risks for those devices. Feedback on how useful the communication considerations outlined in Section 6 may be for consumers and manufacturers, as well as how the considerations can be improved, is particularly important.

Trademark Information

Preface

The overall objective of this publication is to provide voluntary guidance for IoT device manufacturers to help in identifying and planning device cybersecurity features for their products. A key motivation for developing this publication is also to help address the problem of IoT devices being compromised by attackers and joined to botnets, where they can be used to perform distributed denial of service (DDoS) attacks. Use of large numbers of IoT devices in botnets for the Mirai botnet attack in the fall of 2016 highlighted the vulnerable state of many IoT devices.

In 2017, Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, was issued to improve the Nation's cyber posture and capabilities in the face of increasing threats. The Executive Order tasked the Department of Commerce and Department of Homeland Security with leading a process to "…identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)." [1]

The outcome of this joint effort was *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*. [2] Released in May 2018, it identified a number of actions for the IoT ecosystem that should be undertaken. While that report was being developed, NIST had already recognized the need to help organizations understand what cybersecurity risks might be associated with IoT devices. NIST released draft Internal Report (NISTIR) 8228: *Considerations for Managing IoT Cybersecurity and Privacy Risks* in September 2018. [3]

Through related stakeholder engagement and comments received during the NISTIR 8228 public comment period, as well as the contents of the *Report to the President*, NIST identified a critical gap area in guidance on cybersecurity feature baselines[1] for IoT devices. Actions needed to address this gap were included in a November 2018 document, *A Road Map Toward Resilience Against Botnets*. The road map identified tasks and timelines for meeting the objectives in the *Report to the President*. The road map also sequenced the tasks; before assessment, labeling, or awareness initiatives could begin, a core cybersecurity feature baseline that could be considered common across all IoT devices was needed. The road map called on NIST, in collaboration with stakeholders, to define this core cybersecurity feature baseline as a key action to promote raising the basic cybersecurity features of IoT devices and harmonizing across sectors. [5]

This draft document defines the core cybersecurity feature baseline for IoT devices, and it also outlines practices for secure software design and development that can improve the security of IoT devices. This content helps address three of the botnet roadmap tasks: "Define Core Security Capability Baseline,"[2] "Enable Risk Management Approach to IoT Security," and "Publish Best

[1] The term "baseline" should not be confused with the low, moderate, and high control security baselines set forth in NIST Special Publication 800-53 [4] to help federal agencies meet their obligations under the Federal Information Security Modernization Act (FISMA) and other federal policies. In this document, "baseline" is used in the generic sense to refer to a set of foundational requirements or recommendations.

[2] The roadmap referred to "capabilities"; to avoid confusion with the use of "capabilities" in other NIST documents, this publication uses the word "features" instead. The meaning is the same.

Practices for IoT Device Manufacturers." This document also provides the foundation for additional road map tasks to be addressed in the future, especially the creation of extensions of the core baseline targeted at specific use cases with unique challenges.

Call for Patent Claims

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

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

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

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

    i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
    ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

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

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

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

Executive Summary

Manufacturers are creating an incredible variety and volume of Internet of Things (IoT) devices, which incorporate at least one transducer (sensor or actuator) for interacting directly with the physical world, have at least one network interface (e.g., Ethernet, WiFi, Bluetooth, Long-Term Evolution [LTE], ZigBee), and are not conventional IT devices for which the identification and implementation of cybersecurity features is already well understood (e.g., smartphone, laptop). Many IoT devices provide computing functionality, data storage, and network connectivity for equipment that previously lacked these functions. In turn, these functions enable new efficiencies and technological capabilities for the equipment, such as remote access for monitoring, configuration, and troubleshooting. IoT can also add the ability to analyze data about the physical world and use the results to better inform decision making, alter the physical environment, and anticipate future events. [6]

IoT devices are acquired and used by many customers: individuals, companies, government agencies, educational institutions, and other organizations. Unfortunately, IoT devices often lack efficient and effective features for customers to use to help mitigate cybersecurity risks. Consequently, some IoT devices are less easily secured using customers' existing methods because the cybersecurity features they expect may not be available on IoT devices or may function differently than is expected based on conventional IT devices. This means IoT device customers may have to select, implement, and manage additional or new cybersecurity controls or alter the controls they already have. However, new or tailored controls to sufficiently mitigate risks to the same level as before may not be available to all customers or implementable with all IoT devices. Compounding this problem, customers may not know they need to alter their existing IT processes to accommodate IoT. The result is many IoT devices are not secured properly, so attackers can more easily compromise them and use them to harm device customers and conduct additional nefarious acts (e.g., distributed denial of service [DDoS] attacks) against other organizations.[3]

Addressing the challenges of IoT cybersecurity necessitates educating IoT device customers on the differences in cybersecurity risks and risk mitigation for IoT versus conventional IT, as NIST has documented in Internal Report (IR) 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*. [3] The challenges also necessitate educating IoT device manufacturers on how to identify the cybersecurity features customers need IoT devices to have. This includes improving communications between manufacturers and customers regarding device cybersecurity features and related expectations.

This document presents a core baseline of cybersecurity features for all IoT devices that makes devices at least minimally securable by the customers who acquire and use them. This publication does not specify how customers should secure the IoT devices they deploy and use; it only addresses the importance of manufacturers making all IoT devices minimally securable for

[3] In 2017, Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure [1], was issued to improve the Nation's cyber posture and capabilities in the face of intensifying threats. The Executive Order tasked the Department of Commerce and Department of Homeland Security with creating the Enhancing Resilience Against Botnets Report [5] to determine how to stop attacker use of botnets to perform DDoS attacks. This report contained many action items, and this document fulfills two of them: to create a baseline of cybersecurity features for IoT devices, and to publish cybersecurity practices for IoT device manufacturers.

their customers. The core baseline is intended to help customers achieve a basic cybersecurity posture that mitigates general cybersecurity risks. These features are not exhaustive, and IoT device manufacturers are encouraged to use the core baseline as a starting point. Ultimately, by including cybersecurity features in the IoT devices they design and develop, IoT device manufacturers can help enable IoT device customers to effectively manage their cybersecurity risk, as well as strengthening the security of their devices.

Table of Contents

List of Appendices

1 Introduction

1.1 Purpose and Scope

The purpose of this publication is to help improve how securable IoT devices are (e.g., easy for device customers to secure within their systems and environments). IoT device manufacturers will learn how they can help IoT device customers with cybersecurity risk management by carefully considering which cybersecurity features to design into their devices for customers to use in managing their cybersecurity risk.

The publication defines a core baseline of cybersecurity features based on common cybersecurity risk management approaches as a starting point for manufacturers. Manufacturers are encouraged to consider the particular use cases and risks of the systems and environments their devices may be deployed within, in order to move beyond the core baseline to the set of features most appropriate for their devices and customers. The use cases should reflect not only how the devices would be used, but also how attackers might misuse and compromise the devices; the latter has been extensively covered elsewhere and is out of scope for this publication.

IoT device manufacturers will also gain a better understanding of the need to clearly communicate to customers the cybersecurity-relevant characteristics of their IoT devices. This helps customers implement their cybersecurity risk management processes more effectively and efficiently as they incorporate these devices into their systems and environments. Customers can use this publication as a starting point to identify cybersecurity features they want their IoT devices to have and to specify those features to manufacturers as part of procurement efforts.

The scope of this publication is IoT devices that have at least one transducer (sensor or actuator) for interacting directly with the physical world, have at least one network interface (e.g., Ethernet, WiFi, Bluetooth, Long-Term Evolution [LTE], ZigBee), and are not conventional IT devices for which the identification and implementation of cybersecurity features is already well understood (e.g., smartphone, laptop).[4] All other types of devices considered part of the IoT ecosystem are out of scope, but no IoT device operates in isolation. Rather, IoT devices will be used in systems and environments with many other devices and components, some of which may be IoT devices, while others may be conventional IT equipment. Manufacturers should also consider the complexity of how IoT devices interact with other devices, systems, and environments when identifying the cybersecurity features to incorporate into their devices.

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

[4] The usage of the term "baseline" in this document should not be confused with the low, moderate, and high control security baselines set forth in NIST Special Publication (SP) 800-53 [4] to help federal agencies meet their obligations under the Federal Information Security Modernization Act (FISMA) and other federal policies. In this document, "baseline" is used in the generic sense to refer to a set of foundational requirements or recommendations.

1.2 Publication Structure

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

- Section 2 summarizes key points from NIST Internal Report (IR) 8228 that are prerequisites for understanding the rest of this publication.
- Section 3 discusses considerations for IoT device manufacturers when identifying the cybersecurity features their IoT devices will provide, based on the manufacturers' determination of likely cybersecurity risks their device customers will face.
- Section 4 defines the core baseline of cybersecurity features that acts as a starting point for identifying features for IoT devices, as explained in Section 3.
- Section 5 explores considerations for manufacturers implementing cybersecurity features for IoT devices.
- Section 6 explains the need for communication with customers regarding cybersecurity risk mitigation, and provides examples of the types of information to be communicated and how it could vary for different customers.
- Section 7 briefly discusses secure development practices for manufacturers that help improve the security (reduce the prevalence of vulnerabilities) of IoT devices.
- The References section lists the references for the publication.
- Appendix A provides an acronym and abbreviation list.
- Appendix B contains a glossary of selected terms used in the publication.

2 Background

This section summarizes context and key points from NIST IR 8228 [3] that are prerequisites for understanding the rest of this document. Readers who are already familiar with NIST IR 8228 can skip this section. Readers unfamiliar with NIST IR 8228 should be able to use the context provided by this section to understand the rest of this publication, but unfamiliar readers are also encouraged to refer to NIST IR 8228 for more details about these concepts.

Many IoT devices affect cybersecurity risks differently than conventional information technology (IT) devices do (e.g., desktops, laptops, servers), which can be broadly seen through three high-level considerations:

1. **Many IoT devices interact with the physical world in ways conventional IT devices usually do not.** The potential impact of some IoT devices making changes to physical systems and thus affecting the physical world needs to be explicitly recognized and addressed from cybersecurity and privacy perspectives. Also, operational requirements for performance, reliability, resilience, and safety may be at odds with common cybersecurity practices for conventional IT devices.
2. **Many IoT devices cannot be accessed, managed, or monitored in the same ways conventional IT devices can.** This can necessitate doing tasks manually or significantly differently than for conventional IT for some IoT devices, expanding staff knowledge and tools to include a much wider variety of IoT device software, and addressing risks with manufacturers and other third parties having remote access or control over IoT devices.
3. **The availability, efficiency, and effectiveness of cybersecurity features are often different for IoT devices than conventional IT devices.** This means organizations may have to select, implement, and manage additional controls, as well as determine how to respond to risk when sufficient controls for mitigating risk are not available.

Cybersecurity risks for IoT devices can be thought of in terms of two high-level risk mitigation goals:

1. **Protect device security**. In other words, prevent a device from being used to conduct attacks, including participating in DDoS attacks against other organizations, and eavesdropping on network traffic or compromising other devices on the same network segment. This goal applies to all IoT devices.
2. **Protect data security.** Protect the confidentiality, integrity, and/or availability of data (including personally identifiable information [PII]) collected by, stored on, processed by, or transmitted to or from the IoT device. This goal applies to each IoT device except those without any data that needs protection.

Meeting any risk mitigation goal involves addressing a set of risk mitigation areas. Based on an analysis of existing NIST publications such as the Cybersecurity Framework [7] and SP 800-53 [4] and the characteristics of IoT devices, common risk mitigation areas for IoT devices are:

- **Asset Management:** Maintain a current, accurate inventory of all IoT devices and their relevant characteristics throughout the devices' lifecycles in order to use that information for cybersecurity risk management purposes.
- **Vulnerability Management:** Identify and eliminate known vulnerabilities in IoT device software and firmware in order to reduce the likelihood and ease of exploitation and compromise.
- **Access Management:** Prevent unauthorized and improper physical and logical access to, usage of, and administration of IoT devices by people, processes, and other computing devices.
- **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 device operations.
- **Incident Detection:** Monitor and analyze IoT device activity for signs of incidents involving device and data security.

Risk mitigations within these areas carry certain expectations based on conventional IT devices that may not be met or may be met significantly differently for some IoT devices, sometimes in unexpected ways. As a result, there are one or more challenges that IoT devices may pose to each expectation, such as not having expected device features (i.e., technical hardware, software, and firmware functionality). The end result of these linkages is the identification of a structured set of potential challenges with mitigating cybersecurity risk for IoT devices that can each be traced back to the relevant risk considerations.

Figure 1 depicts the relationships among the major NIST IR 8228 concepts: risk considerations, risk mitigation goals and areas, expectations, and challenges. For more information on any of these, see Sections 3 and 4 of NIST IR 8228. [3] This document aims to help manufacturers of IoT devices address gaps in IoT device features relative to conventional IT equipment, which will help reduce challenges by aligning IoT devices better with expectations.

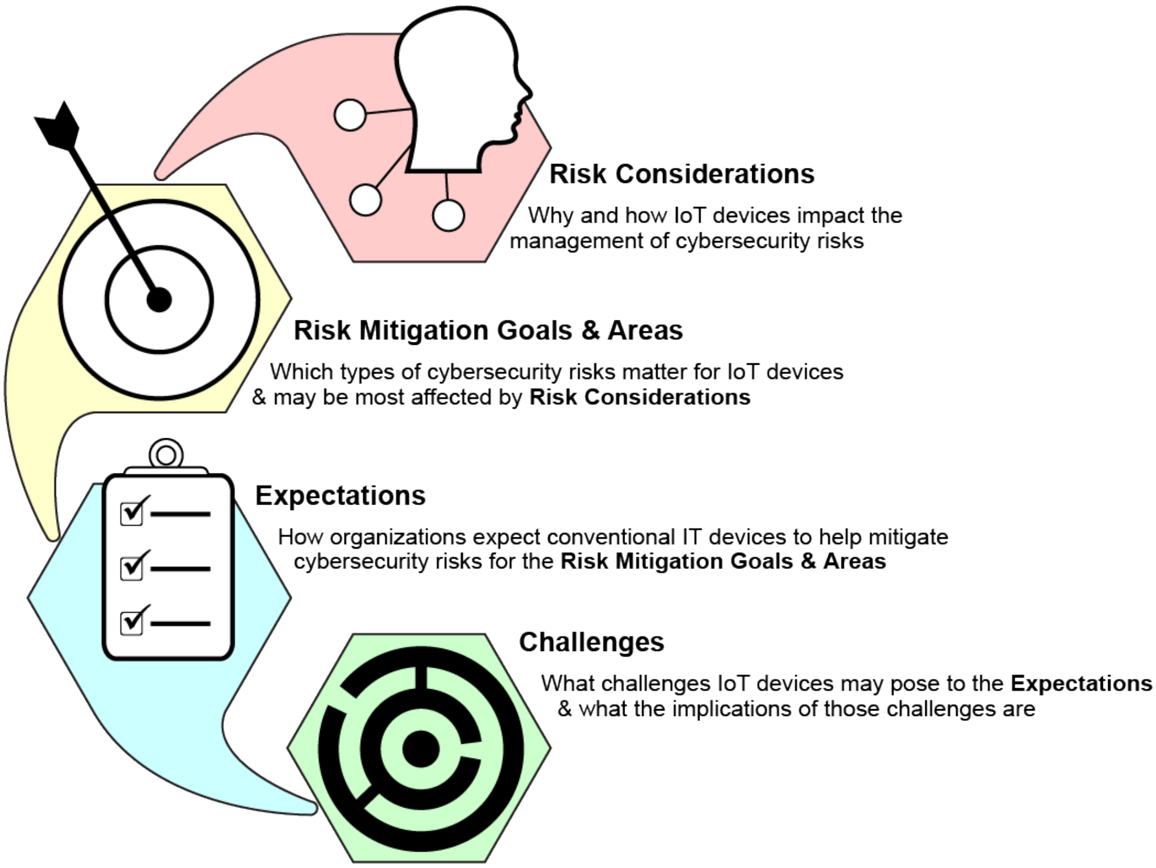

Figure 1: Relationships Among Major NIST IR 8228 Concepts

3 Cybersecurity Feature Identification

This section is intended to help IoT device manufacturers better identify the cybersecurity risks their customers (individuals and organizations) face so IoT devices can provide the cybersecurity features customers need. Manufacturers cannot completely understand all of their customers' risk because every customer, system, and IoT device faces unique risks based on many factors; however, manufacturers can consider the expected use cases for their IoT devices, and then make their devices at least minimally securable by customers who acquire and use them consistent with those use cases. *Minimally securable* means the devices have the technical features (i.e., hardware, firmware, and software) customers may need to implement cybersecurity controls used to mitigate some common cybersecurity risks. Customers are still ultimately responsible for securing their systems and the IoT devices they incorporate, including using additional technical, physical, and procedural means, but cybersecurity features built into IoT devices generally make risk mitigation easier and more effective for customers.

This section and the rest of the publication are intended to inform the existing cybersecurity risk management practices IoT device manufacturers already follow as part of their IoT device design processes. This section does not define a risk management methodology or process, but instead provides additional considerations for manufacturers to be incorporated into existing processes. Section 4 defines a core baseline of cybersecurity features that manufacturers can use as a starting point for identifying the appropriate features for their IoT devices. The goal is for manufacturers to consider cybersecurity risks in the context of the applicable use case or cases for the IoT device so the device's hardware, firmware, and software design can help mitigate those risks.

3.1 Expected Customers and Use Cases

An early step in IoT device design is identifying the expected customers for the device. They could be as broad as every person and organization, or they could be types of people (e.g., musicians, cyclists, chefs, preschoolers) or organizations, such as small retail businesses, large hospitals, energy companies with solar farms, or educational institutions with buses. Identifying expected customers is vital for determining which cybersecurity features an IoT device should implement and how it should implement them. For example, an enterprise might need a device to integrate with its log management servers, but a typical home customer would not.

Another early step in IoT device design is defining use cases for the device based on the expected customers. Each use case should explain how the customers will use the device, where the device will be used (e.g., countries, jurisdictions within countries), what environments the device will be used in (e.g., inside or outside; stationary or moving; public or private; movable or immovable), likely system dependencies, and other aspects of device use that might be relevant to the device's cybersecurity risk. Each use case should also reflect how attackers might misuse and compromise the devices to ensure that is taken into consideration.

3.2 Device Cybersecurity Features

The expected customers and use cases can serve as assumptions for identifying device cybersecurity features. Here are a few examples:

- **Device management**: The method or methods likely to be used by device customers to manage the device, if any, are important to consider. For example, an IoT device intended for enterprise use could support integration with common enterprise systems (e.g., asset management, vulnerability management, log management). If used, this feature would give enterprise customers a greater degree of control and visibility into the devices' cybersecurity risk. For an IoT device expected to be used in home environments only, this feature would not be relevant, and customers would expect a user-friendly way to manage their devices, or even want the manufacturer to perform all device management on their behalf (e.g., installing patches automatically without customer involvement).
- **Configurability:** Configurability is closely related to device management. For example, making a device highly configurable is generally more desirable in enterprise 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 misconfigure a device, weakening its security and increasing the likelihood of a compromise. On the other hand, some configuration settings, such as enabling or disabling clock synchronization services for the device and choosing a time server to use for clock synchronization, may be desired by both enterprise and home customers. Device configuration might be entirely omitted in cases where the device does not need to be provisioned or customized in any way during or after deployment (e.g., does not need to be joined to a wireless network, does not need to be associated with a particular user).
- **Network characteristics**: Devices expected to be used on networks with low bandwidth, unreliable networks, or other networks that significantly impede the flow of network traffic might preclude the use of certain features. For example, depending on such a network for downloading large updates might saturate the network connection, disrupting other usage, and take far too long to get updates to the device. Manufacturers could consider alternative update strategies, such as changing their processes so as to reduce the size of updates, or distributing updates to administrators on high-speed network connections and having the administrators manually transfer the updates to the IoT device (which introduces additional cybersecurity risks from malware being transmitted by removable media that may need to be mitigated).
- **The nature of device data:** There is a great deal of variability across IoT devices when it comes to the nature of the data they collect, process, store, and transmit. Some devices do not store any data, while others store data that could cause significant harm if accessed or modified by unauthorized entities. Understanding the nature of data on a device in the context of the customers and use cases can help manufacturers identify the features needed to protect device data. Examples of possible features include data encryption, device and user authentication, access control, and backup/restore.
- **Access level:** The cybersecurity features an IoT device needs can be greatly affected based on how accessible the device is, either logically or physically. An example is an IoT food vending machine in a public place, which is internet connected so suppliers can track inventory and machine status. Vending machine users would not be required to authenticate themselves in order to insert money and purchase a snack. However, the vending machine would also be highly susceptible to physical attack.

NIST IR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* [3] discusses additional cybersecurity-related considerations that manufacturers should be mindful of when identifying cybersecurity features. It is recommended that IoT device manufacturers read NIST IR 8228 and use the material in Sections 3 and 4 as the basis of identifying the cybersecurity features their devices should provide. Tables 1 and 2 in Section 4 of NIST IR 8228 list common shortcomings in IoT device cybersecurity and explain how they can negatively impact customers. This includes references to Cybersecurity Framework subcategories [7] and NIST SP 800-53 controls [4], which many organizations use when discussing cybersecurity.

Manufacturers should also identify any known requirements in their use cases, such as sector-specific cybersecurity regulations or country-specific laws, so they can be mindful of those requirements during feature identification.

Identifying the cybersecurity features devices need should happen as early in device design processes as feasible so the features can be taken into account when selecting or designing IoT device hardware, firmware, and software. For many IoT devices, additional types of risks, such as privacy,[5] safety, reliability, or resiliency, need to be managed simultaneously with cybersecurity risks because of the effects addressing one type of risk can have on others. A common example is ensuring that when a device fails, it does so in a safe manner. Only cybersecurity risks are in scope for this publication. Readers who are particularly interested in better understanding other types of risks and their relationship to cybersecurity may benefit from reading NIST SP 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security*. [8]

[5] A number of privacy efforts, including the NIST Privacy Framework (https://www.nist.gov/privacy-framework), are currently underway that are likely to inform needed IoT device features to support privacy. While the core baseline includes cybersecurity features that also support privacy, such as protecting the confidentiality of data, it does not include non-cybersecurity features that support privacy.

4 The Core Baseline for IoT Devices

To provide manufacturers a starting point to use in identifying the necessary cybersecurity features for their IoT devices, this section defines a core cybersecurity feature baseline (*core baseline*), which is a set of technical features needed by a generic customer to support common cybersecurity controls that protect the customer's devices and device data, systems, and ecosystems as described in Section 2. The core baseline's role is as a default for minimally securable devices, meaning that cybersecurity features will often need to be added or removed from an IoT device's design to take into account the manufacturer's understanding of customers' likely cybersecurity risks. Also, the core baseline does not specify how the cybersecurity features are to be achieved, so manufacturers who choose to adopt the core baseline for any of the IoT devices they produce have considerable flexibility in implementing it to effectively address customer needs. Section 5 provides additional considerations for feature implementation.

Table 1 defines the cybersecurity features in the core baseline. Each row defines a feature and provides a numbered list of key elements of that feature—elements an IoT device manufacturer seeking to implement the core baseline must meet in order to achieve the feature. (Note: the elements are not intended to be comprehensive, nor are they in any particular order.) The third column explains the rationale for needing the feature and its key elements to be included in the core baseline for the generic case. Finally, the last column lists reference examples that indicate existing sources of IoT device cybersecurity guidance specifying a similar or related cybersecurity feature. Definitions of selected terms from Table 1, the terms that are underlined, are provided after the table.

Each feature and key element in the core baseline stems directly from the contents of Section 4 of NIST IR 8228, and the core baseline addresses the most common issues in IoT devices based on its findings. See NIST IR 8228 for more details on the rationales behind everything in the core baseline. [3]

Table 1: The Core Cybersecurity Feature Baseline for Securable IoT Devices

Feature	Key Elements	Rationale	Reference Examples
Device Identification: The IoT device can be uniquely identified logically and physically.	1. A unique logical identifier 2. A unique physical identifier on it at an external or internal location authorized entities can access Note: the physical and logical identifiers may represent the same value, but they do not have to.	• This feature supports asset management, which in turn supports vulnerability management, access management, data protection, and incident detection. • The unique logical identifier can be used to distinguish the device from all others, usually for automated device management and monitoring. The unique logical identifier can also be used for device authentication. • The unique physical identifier can be used to distinguish the device from all others whenever the unique logical identifier is unavailable, such as during device deployment and decommissioning, or after a device failure.	• **BITAG** [9]: 7.2, 7.6 • **CTIA** [10]: 4.13 • **ENISA** [11]: PS-10, TM-21 • **GSMA** [12]: CLP11_5.2.1, CLP13_6.6.2, 6.8.1, 6.20.1, 8.11.1 • **IIC** [13]: 7.3, 8.5, 11.7, 11.8 • **IoTSF** [14]: 2.4.8.1, 2.4.14.3, 2.4.14.4
Device Configuration: The IoT device's software and firmware configuration can be changed, and such changes can be performed by authorized entities only.	1. The ability to change the device's software and firmware configuration settings 2. The ability to restrict configuration changes to authorized entities only 3. The ability for authorized entities to restore the device to a secure default configuration defined by an authorized entity	• This feature supports vulnerability management, access management, data protection, and incident detection. • Customers often want to alter a device's configuration for a variety of reasons, including cybersecurity, interoperability, privacy, and usability. Without a device configuration feature, a customer can only use a device as-is and cannot customize it to meet the customer's needs, integrate the device into the customer's environment, etc. • Most cybersecurity features are at least somewhat dependent on the presence of a device configuration feature. • Unauthorized entities may want to change a device's configuration for many reasons, such as gaining unauthorized access, causing the device to malfunction, or secretly monitoring the device's environment. • The ability to restore a secure default configuration for a device is helpful when the current configuration contains errors, has been damaged or corrupted, or is otherwise no longer thought to be trustworthy.	• **BITAG**: 7.1, 7.2 • **CSA2** [15]: 22 • **CTIA**: 4.7, 4.8, 4.12, 5.15 • **GSMA**: CLP12_5.3.1.3, 5.6.2 • **IIC**: 7.3, 7.6, 8.10, 11.1, 11.2, 11.5 • **IoTSF**: 2.4.7.7, 2.4.8, 2.4.15

Feature	Key Elements	Rationale	Reference Examples
Data Protection: The IoT device can protect the data it stores and transmits from unauthorized access and modification.	1. The ability to use accepted cryptographic modules for standardized cryptographic algorithms (e.g., encryption with authentication, cryptographic hashes, digital signature validation) to prevent the confidentiality and integrity of the device's stored and transmitted data from being compromised 2. The ability for authorized entities to configure the cryptography use itself when applicable, such as choosing a key length 3. The ability for authorized entities to render all data on the device inaccessible by all entities, whether previously authorized or not (e.g., through a wipe of internal storage, destruction of cryptographic keys for encrypted data)	• This feature supports access management, data protection, and incident detection. • Customers often want the confidentiality of their data protected so unauthorized entities cannot access their data and misuse it. • Customers often want the integrity of their data protected so it is not inadvertently or intentionally changed, which could have a variety of adverse consequences (e.g., issuing the wrong command to a piece of equipment, concealing malicious activity).	• **AGELIGHT** [16]: 5, 7, 18, 24, 25, 34 • **BITAG**: 7.2, 7.10 • **CTIA**: 4.8, 4.10, 5.15 • **ENISA**: GP-OP-04, GP-TM-14, GP-TM-24, GP-TM-32, GP-TM-34, GP-TM-35, GP-TM-36, GP-TM-39, GP-TM-40 • **ETSI** [17]: 4.4-1, 4.5-1, 4.5-2, 4.11-1, 4.11-2, 4.11-3 • **GSMA**: CLP12_5.1.5, 5.1.7.1, 5.2.2.1, 5.3.1.1, 6.2.1, 6.3.1.2, CLP13_6.1.1.6, 6.1.1.8, 6.4.1.1, 6.5.1.1, 6.11, 6.12.1.1, 7.6.1, 8.10.1.1, 8.11.1 • **IIC**: 7.3, 7.4, 7.7, 8.8, 8.11, 8.13, 9.1 • **IoTSF**: 2.4.5, 2.4.7, 2.4.8.8, 2.4.8.16, 2.4.9, 2.4.12.2, 2.4.12.11, 2.4.13.16, 2.4.16.1, 2.4.16.2
Logical Access to Interfaces: The IoT device can limit logical access to its local and network interfaces to authorized entities only.	1. The ability to logically or physically disable any local and network interfaces that are not necessary for the core functionality of the device 2. The ability to logically restrict access to each network interface (e.g., device authentication, user authentication) 3. The ability to enable, disable, and adjust thresholds for any ability the device might have to lock or disable an account or to delay additional authentication attempts after too many failed authentication attempts	• This feature supports vulnerability management, access management, data protection, and incident detection. • Limiting access to interfaces reduces the attack surface of the device, giving attackers fewer opportunities to compromise it. For example, unrestricted network access to an IoT device enables attackers to directly interact with the device, which significantly increases the likelihood of the device being compromised.	• **AGELIGHT**: 10, 13, 14, 18, 39 • **BITAG**: 7.1, 7.2, 7.3 • **CTIA**: 3.2, 3.3, 3.4, 4.2, 4.3, 4.9, 5.2 • **ENISA**: GP-TM-08, GP-TM-09, GP-TM-21, GP-TM-22, GP-TM-27, GP-TM-29, GP-TM-33, GP-TM-42, GP-TM-44, GP-TM-45 • **ETSI**: 4.1-1, 4.4-1, 4.6-1, 4.6-2 • **GSMA**: CLP12_5.6.1, 6.3.1.1, 7.1.1.2, CLP13_6.12.1, 7.10.1, 8.2.1.1 • **IIC**: 7.3, 7.4, 8.3, 8.6, 11.7 • **IoTSF**: 2.4.4.5, 2.4.5, 2.4.6, 2.4.7, 2.4.8, 2.4.13, 2.4.15

Feature	Key Elements	Rationale	Reference Examples
Software and Firmware Update: The IoT device's software and firmware can be updated by authorized entities only using a secure and configurable mechanism.	1. The ability to update all the device's software and firmware through remote (e.g., network download) and/or local means (e.g., removable media) 2. The ability to confirm the validity of any update before installing it 3. The ability to restrict updating actions to authorized entities only 4. The ability to enable or disable updating 5. The ability to set remote update mechanisms to be either automatically or manually initiated for update downloads and installations 6. The ability to enable or disable notification when an update is available and specify who or what is to be notified	• This feature supports vulnerability management. • Updates can remove vulnerabilities from an IoT device, which lowers the likelihood of an attacker compromising the device. • Updates can correct IoT device operational problems, which can improve device availability, reliability, performance, and other aspects of device operation.	• **AGELIGHT**: 1, 2, 4 • **BITAG**: 7.1 • **CTIA**: 3.5, 3.6, 4.5, 4.6, 5.5, 5.6 • **ENISA**: GP-TM-18, GP-TM-19 • **ETSI**: 4.3-1, 4.3-2, 4.3-7 • **GSMA**: CLP11_5.3.3, CLP12_5.8.1, 5.9.1.3, 6.6.1 • **IIC**: 7.3, 11.5.1 • **IoTSF**: 2.4.5, 2.4.6, 2.4.13.1
Cybersecurity Event Logging: The IoT device can log cybersecurity events and make the logs accessible to authorized entities only.	1. The ability to log cybersecurity events across the device's software and firmware 2. The ability to record sufficient details for each event to facilitate an authorized entity examining the log and determining what happened 3. The ability to restrict access to the logs so only authorized entities can view them 4. The ability to prevent any entities (authorized or unauthorized) from editing the logs 5. The ability to make the logs available to a logging service on another device, such as a log server	• This feature supports vulnerability management and incident detection. • Cybersecurity event logging provides a record of events that can be useful in investigating compromises, identifying misuse, and troubleshooting certain operational problems.	• **CTIA**: 4.7, 4.12, 5.7 • **ENISA**: GP-TM-55 • **ETSI**: 4.10-1 • **GSMA**: CLP11_5.3.4, CLP12_5.7.1.2, 5.7.1.3, CLP13_6.13.1, 7.2.1, 9.1.1.2 • **IIC**: 7.3, 7.5, 7.7, 8.9, 10.3, 10.4

Definitions of selected terms from the table are as follows:

- An *authorized entity* is an entity that has implicitly or explicitly been granted approval to interact with a particular IoT device. The core baseline features do not specify how authorization is implemented for distinguishing authorized and unauthorized entities. It is left to the manufacturer to decide how each device will implement authorization.

- *Configuration* is "the possible conditions, parameters, and specifications with which an information system or system component can be described or arranged." [18] The Device Configuration feature does not define which configuration settings should exist, simply that a mechanism to manage configuration settings exists.
- *Cybersecurity events* are observable occurrences with cybersecurity significance in an IoT device. (This definition is derived from [4].)
- A *device identifier* is a context-unique value that is associated with a device (for example, a string consisting of a network address). (This definition is derived from [19].)
- An *entity* is a person, device, service, network, domain, manufacturer, or other party who might interact with an IoT device.
- *Firmware* is "computer programs and data stored in hardware[…]such that the programs and data cannot be dynamically written or modified during execution of the programs." [4]
- An *interface* is a boundary between the IoT device and entities where interactions take place. (This definition is derived from [20].) There are two types of interfaces: network and local.
- *Local interfaces* are interfaces that can only be accessed physically, such as ports (e.g., USB, audio, video/display, serial, parallel, Thunderbolt) and removable media drives (e.g., CD/DVD drives, memory card slots).
- *Local logical access* is logical access to an IoT device that does not occur over a network.
- A *logical identifier* is a device identifier that is expressed logically by the device's software or firmware. An example is a media access control (MAC) address assigned to a network interface.
- *Network interfaces* are interfaces that connect the IoT device to networks.
- A *physical identifier* is a device identifier that is expressed physically by the device (e.g., printed onto a device's housing, displayed on a device's screen).
- *Remote logical access* is logical access to an IoT device that occurs over a network.
- *Software* is "computer programs and associated data that may be dynamically written or modified during execution." [4]
- An *update* is a patch, upgrade, or other modification to code that corrects security and/or functionality problems in software or firmware. (This definition is derived from [21].)

5 Cybersecurity Feature Implementation

Manufacturers should implement cybersecurity features in ways that will be appropriate for their customers. Two important aspects of feature implementation are defining the specifications for the IoT device hardware, firmware, and software, and understanding how an IoT device may inherit cybersecurity features from the system or environment it is deployed within. This section discusses these aspects in more detail.

5.1 Device Specifications

Manufacturers properly provisioning device hardware, firmware, and supporting software to provide the necessary cybersecurity features will help make the devices more securable. The following considerations for manufacturers are suggestions and are not comprehensive:

- Select or build a device with sufficient hardware resources (e.g., processing, memory, storage, network technology, power), as well as firmware and software resources, to support the desired features. For example, encryption is processing-intensive, and a device with limited processing might not be able to support encryption that customers need. Some devices cannot support the use of an operating system or Internet Protocol (IP) networks.
- Be forward-looking and size hardware resources for potential future use. As an example, if a device has a 10-year lifespan, it may be necessary to update the encryption algorithm or key length the device uses, and the new algorithm or key length may make encryption more processing-intensive.
- Use hardware-based cybersecurity features. An example is having a hardware root of trust that provides trusted storage for cryptographic keys and enables performing secure boots and confirming device authenticity.
- Do not include unneeded features provided by hardware, firmware, and/or the operating system; if the inclusion of such features cannot be avoided, ensure they can be disabled to prevent misuse and exploitation. For example, if a device has local interfaces on its external housing and the device is likely to be deployed in public areas, possible approaches include offering a tamper-resistant enclosure to prevent physical access to the interfaces, and offering a configuration option that logically disables the interfaces.
- Do not force the use of features that may negatively impact operations. A classic example is authentication. Features intended to deter brute force attacks against passwords, such as locking out an account after too many failed authentication attempts, can inadvertently cause a denial of service for the person or device attempting to authenticate. In safety-critical environments, for example, such disruptions to access may not be acceptable because of the danger they would cause. Customers often need flexibility in configuring such features or disabling them altogether.

Manufacturers may want to consider using an established IoT platform instead of acquiring and integrating hardware, firmware, and supporting software components (e.g., operating system). An *IoT platform* is a piece of IoT device hardware with firmware and/or 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 (SDK) to help expedite IoT application development. Manufacturers can choose an adequately resourced IoT platform instead of designing hardware, installing and configuring an operating system or firmware, creating new cloud-based services, writing IoT device applications and mobile apps from scratch, and performing other tasks that are error-prone and generally more likely to introduce new vulnerabilities into the IoT device compared to adopting an established platform.

Whether or not an IoT platform is being used for a device, manufacturers should carefully consider the current status and expected lifespan of any third-party components or services before including them in the IoT device design. Avoid using any hardware, firmware, or software that is no longer maintained.

5.2 Cybersecurity Feature Inheritance

IoT device design processes may determine that certain cybersecurity features can be omitted from IoT devices because equivalent protection will be inherited from elsewhere. For example, if an IoT device is intended for use in an environment with stringent physical security controls in place, a manufacturer might be able to omit restricting access to the device's local interfaces because the facility's physical security can take care of it. On the other hand, an IoT device with a particularly important function might merit keeping cybersecurity features for local interface access restriction in order to provide an additional layer of security against attacks.

Another example of cybersecurity inheritance is an IoT device being dependent on an IoT gateway or hub for its communications. Such an IoT device cannot fully function unless it communicates directly with an IoT gateway or hub within its physical or logical proximity, with the gateway or hub acting as an intermediary between the IoT device and other devices or services. "IoT gateway" and "IoT hub" are terms without consistent definitions as of this writing, but what matters is the functionality the gateway or hub provides, not the term used. Most IoT gateways and hubs provide one or both of the following: 1) networking services that connect two networks, usually with different protocols, and restrict the traffic between the two networks; and 2) application services that provide command and control functionality for IoT devices.

An IoT device that is properly shielded from devices outside its network by an IoT gateway or hub can only be accessed in one of two ways—through the IoT gateway or hub, or within physical proximity of the device—so that IoT device effectively inherits network logical access protection from the IoT gateway or hub. An IoT gateway or hub with application services might also be able to handle cybersecurity event logging for an IoT device, especially if the IoT device's internal cybersecurity events are not deemed significant enough to merit logging. Dependency on an IoT gateway/hub has other positive security implications, such as a greater chance of malicious activity involving the IoT device being detected (because its network traffic passes through the IoT gateway/hub). However, shifting features from the IoT device to an IoT gateway or hub makes the cybersecurity of that gateway or hub critical to the cybersecurity of the IoT device.

A final group of examples involves device identifiers. An IoT device fully contained within another IoT device might inherit certain cybersecurity features from the outer device, such as the outer device's unique logical and physical device identifiers. An IoT device that will be deployed in an environment without physical access to the device, such as sensors embedded within a structure or a substance, may not need a physical device identifier because the environment around it provides unique identification for it.

These examples help illustrate why the core baseline of cybersecurity features is not intended to be fully adopted by every IoT device; every IoT device has a unique set of expected customers and use cases, and not all features in the core baseline will make sense to use in every situation. It is important that manufacturers explain to customers, in sufficient detail, why any core baseline features have been omitted from an IoT device so customers are aware the features are absent and understand the rationale.

6 Cybersecurity Information to Provide to Customers

Many customers will benefit from manufacturers communicating to them more clearly about cybersecurity risks involving their IoT devices. This section provides examples of information that may be particularly beneficial to communicate to customers, especially in enterprise environments. These examples are not unique to IoT, and they will not necessarily apply to all IoT devices a manufacturer produces. However, the information is supportive of and particularly applicable to IoT cybersecurity, and is likely to address cybersecurity challenges currently affecting many IoT devices and customers.

Manufacturers should strive to present this information to customers as clearly as possible, in terms the customer will understand, and in logical and physical locations the customer will see or hear it and can readily locate it again whenever needed. Achieving this may require a different approach for different kinds of customers based on their expectations and resources. In some instances, this may mean presenting more or less information based on the customer targeted and their needs.

Device Cybersecurity Features: Communicating to customers which cybersecurity features the device provides, especially using common terminology (e.g., the feature names from the core baseline), and how these features may affect risk helps customers better understand how to manage risk for the device. Similarly, if features customers would expect to be provided by the device are not, it would help if the missing features were identified as such so customers could adjust their risk management accordingly. Manufacturers should also explain why the features were not included.

For most customers, information on device cybersecurity features is likely to be more useful if it includes an explanation of the assumptions the manufacturer made, such as how the device will be used, what type of environment it will be used in, what cybersecurity features will be inherited from elsewhere (e.g., an IoT gateway), and how responsibilities are expected to be shared among the manufacturer, the customer, and others.

Device Transparency: Communicating to customers information about the device's software, firmware, hardware, services, functions, and data types helps customers better understand and manage cybersecurity for their devices, particularly if the customer is expected to play a substantial role in managing device cybersecurity. Important information for customers includes:

- Usable information on cybersecurity-related aspects of the device, including device installation, configuration, usage, management, maintenance, and disposal. This information should include the effect on the device if the cybersecurity configuration is made more restrictive than the secure default (e.g., losing some device functionality).
- An inventory of the IoT device's current internal software and firmware, including versions, patch status, and known vulnerabilities. The ability to inventory the IoT device's internal software and firmware could be offered as a device feature.
- A list of sources of all of the IoT device's software, firmware, hardware, and services.

- Sufficient information on the IoT device's operational characteristics so they can adequately secure the device (e.g., make information on characteristics available on a website; use a standard protocol so devices can provide basic information to authorized parties).
- A list of the functions the IoT device performs (i.e., the device should not perform any hidden functions customers would not expect or want).
- A list of data types the IoT device may collect and the identities of all third parties that can access that data.
- The identities of all parties (including the manufacturer) who have access to or any degree of control over the IoT device.

Software and Firmware Update Transparency: Manufacturers communicating expectations about when updates may be released and who is responsible for performing updates, as well as providing information on the contents of each update, helps customers plan their cybersecurity mitigations and maintain the cybersecurity of their devices, particularly in response to emerging threats. Practices include:

- Set customer expectations on if and when updates will be made available.
- Define the circumstances under which updates will be issued (e.g., controlling execution of faulty software, identification of previously unknown vulnerabilities in protocols).
- Either inform the customer which entity (e.g., customer, manufacturer, third party) is responsible for performing updates, or give the customer the option to designate who will be responsible.
- Notify the customer if installing an update may alter existing configuration settings.
- Notify the customer or the customer's IoT device of update availability and contents (e.g., altered or new functions or features).

Support and Lifespan Expectations: Communicating to customers the length of time a manufacturer intends to support a device and how long the device may be able to function helps customers plan their cybersecurity mitigations throughout the device's support lifecycle, which may be shorter than how long the customer wants to use the device. Practices include:

- State the timeframe for the end of product support.
- State the timeframe for product end-of-life.
- Inform customers of what functionality, if any, the device will have after support ends and at end-of-life.

Decommissioning: Communicating to customers the options, if any, for securely decommissioning a device helps customers plan for securely disposing of devices. Practices include:

- Provide customers sufficient information on whether the IoT device can be decommissioned and how they can decommission it, such as removing all user and configuration data from the device and associated systems (e.g., cloud-based services used by the device), rendering the device inoperable, or transferring ownership to another party.

It is also important for manufacturers to keep the cybersecurity information they communicate to customers easily accessible and up to date. Accessibility includes communicating in language customers will understand. For example, a home user will likely have less technical knowledge than enterprise customer points of contact (e.g., a system administrator), so messages to these different groups should take that into account to avoid confusion. The amount and focus of information may also vary between customers since they will have different needs, preferences, and abilities, with some customers requiring less information than others about various aspects of their devices and features. How customers are contacted may also vary by customer and by device. For some devices, customers, and use cases, it may be more efficient and effective to have some of the information and notifications of changes come directly from the IoT devices or connected interfaces (e.g., smartphone app) instead of mailing lists and other means.

Keeping customers up to date means notifying them of significant changes to previously communicated information. The same recommendations for messaging discussed above apply for follow-up communications, but extra care should be taken to avoid too many or contradictory follow-up messages, which could lead some customers, particularly home customers, to ignore important messages.

7 Secure Development Practices for IoT Devices

The previous sections of this publication have focused on what manufacturers can do to make devices minimally securable. This section covers a different topic: manufacturers improving how secure their IoT devices are by following secure software development practices. Although this does not directly improve how securable devices are for customers, it can improve the security of deployed devices in ways that customers cannot. As a recent NIST white paper, *Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)* [22] states, following secure software development practices should help manufacturers "reduce the number of vulnerabilities in released software, mitigate the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and address the root causes of vulnerabilities to prevent future recurrences."

There are many existing standards, guidelines, and other publications on secure software development. IoT device manufacturers interested in more information can consult the NIST white paper on secure software development [22] 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. Manufacturers looking for information on secure software development can use the references as a starting point.

All of the white paper's practices are relevant for IoT devices, but some are particularly noteworthy, especially for IoT device software developers who are relatively new to cybersecurity:

- Manufacturers ensuring their workforce has the necessary skills to securely develop IoT devices will help manufacturers more easily design and produce such devices. SSDF practices:
    - PO.2, Implement Roles and Responsibilities
- Manufacturers taking steps to protect code and give customers the ability to verify software integrity helps prevent IoT devices from executing malicious code. SSDF practices:
    - PS.1, Protect All Forms of Code from Unauthorized Access and Tampering
    - PS.2, Provide a Mechanism for Verifying Software Release Integrity
    - PS.3, Archive and Protect Each Software Release
- Manufacturers taking steps to reduce vulnerabilities in IoT devices will make devices inherently more secure and reduce the number of vulnerabilities that need to be mitigated by customers. This includes both the initial development of IoT device software and all updates made to the software after its release. SSDF practices:
    - PW.3, Verify Third-Party Software Complies with Security Requirements
    - PW.4, Reuse Existing, Well-Secured Software When Feasible Instead of Duplicating Functionality
    - PW.5, Create Source Code Adhering to Secure Coding Practices

  - PW.7, Review and/or Analyze Human-Readable Code to Identify Vulnerabilities and Verify Compliance with Security Requirements
  - PW.8, Test Executable Code to Identify Vulnerabilities and Verify Compliance with Security Requirements
  - PW.9, Configure the Software to Have Secure Settings by Default
- Manufacturers accepting and responding to vulnerability reports helps customers maintain the cybersecurity of their IoT devices as new threats emerge. SSDF practices:
  - RV.1, Identify and Confirm Vulnerabilities on an Ongoing Basis
  - RV.2, Assess and Prioritize the Remediation of All Vulnerabilities
  - RV.3, Analyze Vulnerabilities to Identify Their Root Causes

778 # 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] Department of Commerce and Department of Homeland Security (2018) A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats. (Department of Commerce and Department of Homeland Security, Washington, DC). https://csrc.nist.gov/CSRC/media/Publications/white-paper/2018/05/30/enhancing-resilience-against-botnets--report-to-the-president/final/documents/eo_13800_botnet_report_-_finalv2.pdf

[3] 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

[4] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[5] Department of Commerce (2018) A Road Map Toward Resilience Against Botnets. (Department of Commerce, Washington, DC). https://www.commerce.gov/sites/default/files/2018-11/Botnet%20Road%20Map%20112918%20for%20posting_0.pdf

[6] Simmon E (forthcoming) A Model for the Internet of Things (IoT). (National Institute of Standards and Technology, Gaithersburg, MD).

[7] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[8] Stouffer K, Pillitteri V, Lightman S, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev 2. https://doi.org/10.6028/NIST.SP.800-82r2

[9] Broadband Internet Technical Advisory Group (BITAG) (2016) Internet of Things (IoT) Security and Privacy Recommendations. (Broadband Internet Technical Advisory Group (BITAG), Denver, CO). https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

[10] CTIA (2018) CTIA Cybersecurity Certification Test Plan for IoT Devices, Version 1.0.1. (CTIA, Washington, DC). https://www.ctia.org/about-ctia/test-plans/

[11] European Union Agency for Network and Information Security (ENISA) (2017) Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures. (European Union Agency for Network and Information Security (ENISA), Athens, Greece). https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[12] Groupe Spéciale Mobile Association (GSMA) (2017) GSMA IoT Security Assessment. (Groupe Spéciale Mobile Association (GSMA), London, UK). https://www.gsma.com/iot/iot-security-assessment/

[13] Industrial Internet Consortium (IIC) (2016) Industrial Internet of Things Volume G4: Security Framework. (Industrial Internet Consortium (IIC), Needham, MA). https://www.iiconsortium.org/IISF.htm

[14] IoT Security Foundation (IoTSF) (2017) IoT Security Compliance Framework, Release 1.1. (IoT Security Foundation (IoTSF), Livingston, Scotland). https://www.iotsecurityfoundation.org/best-practice-guidelines/

[15] Cloud Security Alliance (CSA) IoT Working Group (2015) Identity and Access Management for the Internet of Things. (Cloud Security Alliance (CSA)). https://cloudsecurityalliance.org/download/identity-and-access-management-for-the-iot/

[16] AgeLight Digital Trust Advisory Group (2019) IoT Safety Architecture & Risk Toolkit (IoTSA) v3.1. (AgeLight Advisory & Research Group, Bellevue, WA). http://agelight.com/iot.html

[17] European Telecommunications Standards Institute (ETSI) (2019) Cyber Security for Consumer Internet of Things. ETSI Technical Specification 103 645 V1.1.1. (European Telecommunications Standards Institute (ETSI), Sophia Antipolis Cedex, France). https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

[18] Johnson A, Dempsey K, Ross R, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128. https://doi.org/10.6028/NIST.SP.800-128

[19] Barker E, Chen L, Roginsky A, Vassilev A, Davis R (2019) Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56A, Rev. 3. https://doi.org/10.6028/NIST.SP.800-56Ar3

[20] Committee on National Security Systems (2015) Committee on National Security Systems (CNSS) Glossary. (National Security Agency, Ft. Meade, MD), CNSS Instruction (CNSSI) No. 4009.

[21] Souppaya M, Scarfone K (2013) Guide to Enterprise Patch Management Technologies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 3. https://doi.org/10.6028/NIST.SP.800-40r3

[22] Dodson D, Souppaya M, Scarfone K (2019) Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF). (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Cybersecurity White Paper. https://csrc.nist.gov/CSRC/media/Publications/white-paper/2019/06/07/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft/documents/ssdf-for-mitigating-risk-of-software-vulns-draft.pdf

Appendix A—Acronyms and Abbreviations

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

BITAG	Broadband Internet Technical Advisory Group
CD	Compact Disc
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CSA	Cloud Security Alliance
DDoS	Distributed Denial of Service
DVD	Digital Video Disc
ENISA	European Union Agency for Network and Information Security
ETSI	European Telecommunications Standards Institute
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
GSMA	Groupe Spéciale Mobile Association
ICS	Industrial Control System
IIC	Industrial Internet Consortium
IoT	Internet of Things
IoTSA	Internet of Things Safety Architecture & Risk Toolkit
IoTSF	Internet of Things Security Foundation
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
PII	Personally Identifiable Information
SDK	Software Development Kit
SP	Special Publication
SSDF	Secure Software Development Framework
USB	Universal Serial Bus
WiFi	Wireless Fidelity

Appendix B—Glossary

Selected terms used in this document are defined below.

Actuator	A portion of an IoT device capable of changing something in the physical world. [3]
Authorized Entity	An entity that has implicitly or explicitly been granted approval to interact with a particular IoT device.
Configuration	"The possible conditions, parameters, and specifications with which an information system or system component can be described or arranged." [18]
Core Baseline	A set of technical features needed by a generic customer to support common cybersecurity controls that protect the customer's devices and device data, systems, and ecosystems
Core Cybersecurity Feature Baseline	See *core baseline*.
Cybersecurity Event	An observable occurrence with cybersecurity significance in an IoT device. (derived from [4])
Device Identifier	A context-unique value that is associated with a device (for example, a string consisting of a network address). (derived from [19])
Entity	A person, device, service, network, domain, manufacturer, or other party who might interact with an IoT device.
Firmware	"Computer programs and data stored in hardware[…]such that the programs and data cannot be dynamically written or modified during execution of the programs." [4]
Interface	A boundary between the IoT device and entities where interactions take place. (derived from [20])
IoT Platform	A piece of IoT device hardware with firmware and/or 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.
Local Interface	An interface of an IoT device that can only be accessed physically, such as a port or a removable media drive.
Local Logical Access	Logical access to an IoT device that does not occur over a network.
Logical Identifier	A device identifier that is expressed logically by the device's software or firmware.
Minimally Securable IoT Device	An IoT device that has the technical features (i.e., hardware, firmware, and software) customers may need to implement cybersecurity controls used to mitigate some common cybersecurity risks.

Network Interface	An interface that connects an IoT device to a network (e.g., Ethernet, WiFi, Bluetooth, Long-Term Evolution [LTE], ZigBee).
Physical Identifier	A device identifier that is expressed physically by the device (e.g., printed onto a device's case, displayed on a device's screen).
Remote Logical Access	Logical access to an IoT device that occurs over a network.
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. [3]
Software	"Computer programs and associated data that may be dynamically written or modified during execution." [4]
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. [3]
Update	A patch, upgrade, or other modification to code that corrects security and/or functionality problems in software or firmware. (derived from [21])